Wireless 150 Router

Model # AR570W

User's Manual

Ver. 1A

Federal Communication Commission Interference Statement

FCC Part 15

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio technician for help.

FCC Caution

This equipment must be installed and operated in accordance with provided instructions and a minimum 20 cm spacing must be provided between computer mounted antenna and person's body (excluding extremities of hands, wrist and feet) during wireless modes of operation.
This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.
Any changes or modifications not expressly approved by the party responsible for compliance could void the authority to operate equipment.

Federal Communication Commission (FCC) Radiation Exposure Statement

This equipment complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20cm (8 inches) during normal operation.
The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
The equipment version marketed in US is restricted to usage of the channels 1-11 only.

Table of Contents

FEDERAL COMMUNICATION COMMISSION INTERFERENCE STATEMENT 2

TABLE OF CONTENTS 3

CHAPTER 1 INTRODUCTION 6

1.1 FEATURES 6

1.2 PACKAGE CONTENTS 6

1.3 ROUTER INTERFACE 6

CHAPTER 2 CONNECTING THE ROUTER 9

2.1 BUILDING NETWORK CONNECTION 9

2.2 CONFIGURING THE ROUTER – SETUP WIZARD 9

2.3 CONNECTING TO THE ROUTER WIRELESSLY 21

2.4 TROUBLESHOOTING 24

CHAPTER 3 USING WEB CONFIGURATION UTILITY 25

3.1 NETWORK 26

3.1.1 WAN 26

3.1.2 LAN 26

3.1.3 NAT / Static Routing 29

3.1.4 DDNS 31

3.2 WIRELESS 33

3.2.1 Basic Settings 33

3.2.2 Wireless Security 34

3.2.2.1 WEP 36

3.2.2.2 WPA Pre-share Key 36

3.2.2.3 WPA RADIUS 37

3.2.3 MAC Control 38

3.2.4 Advanced Settings 40

3.2.5 WPS 42

3.3 APPLICATION & GAMING 46

3.3.1 Virtual Server (Port Forwarding) 46

3.3.2 Special Applications (Port Triggering) 47

3.3.3 DMZ 49

3.3.4 ALG Settings 51

3.3.5 QoS 52

3.3.5.1 Add a new QoS rule 53

3.4 ACCESS RESTRICTIONS 56

3.4.1 IP & Port Filtering 56

3.4.2 MAC Filtering 58

3.4.3 URL/Keyword Filtering 60

3.5 SECURITY 62

3.5.1 Firewall 62

3.5.2 DoS (Denial-of-Service) 63

3.5.2.1 DoS – Advanced Settings 63

3.5.3 VPN Pass through 65

3.6 ADMINISTRATION 66

3.6.1 Time 66

3.6.2 Management 67

3.6.2.1 Password 67

3.6.2.2 UPnP 68

3.6.2.3 Reset (Reboot) *68*
3.6.3 Remote Management *69*
3.6.4 Firmware Upgrade *70*
3.6.5 Configuration Settings *71*
3.6.6 Log *72*
3.6.7 Statistics *73*
3.7 STATUS 74
3.7.1 Internet Connection Status *74*
3.7.2 LAN Status *74*
3.7.3 WLAN (Wireless LAN) Status *74*
3.7.4 System Status *75*
TECHNICAL SUPPORT 76

Chapter 1 Introduction

Congratulations on your purchase of Airlink101 Wireless 150 Router AR570W. This product is ideal for home or SOHO users who need greater bandwidth and higher speed for various networking applications, such as VoIP phone, online gaming or online video/audio streaming. Based on Wireless N technology, the data throughput is up to 4 times faster than Wireless G. It is recommended to use with AirLink101® Wireless N or Wireless 150 adapters to reach the best performance.
A full range of security features such as WEP, WPA-PSK, and WPA2-PSK provide the highest level of wireless network security. The web-based Setup Wizard allows you to set up the router with an easy-to-use user interface. Best of all, Wireless 150 Router works with IEEE 802.11 b/g/n network devices, which ensures compatibility with your existing network products.

1.1 Features

- Based on Wireless N technology, 4 times faster than 802.11g*
- Highest data rate of up to 150Mbps* when connected with Airlink101 Wireless N or Wireless 150 Wireless adapters
- Fully compatible with 802.11 b/g/n wireless devices
- Stable wireless connection and high bandwidth enable you to enjoy the network applications without any interruption
- Advanced wireless security WPA2 and WPA to ensure the safety of your network.
- NAT+SPI firewall provides fully protection for your wireless connection
- Easy Setup Button for easy connection to existing wireless network
- QoS (Quality of Service) designed for prioritizing various data traffic to allow downloading files and playing movies, music, or online gaming at the same time

1.2 Package Contents

Before you start to use this router, please check if there's anything missing in the package, and contact your dealer of purchase to claim for missing items:

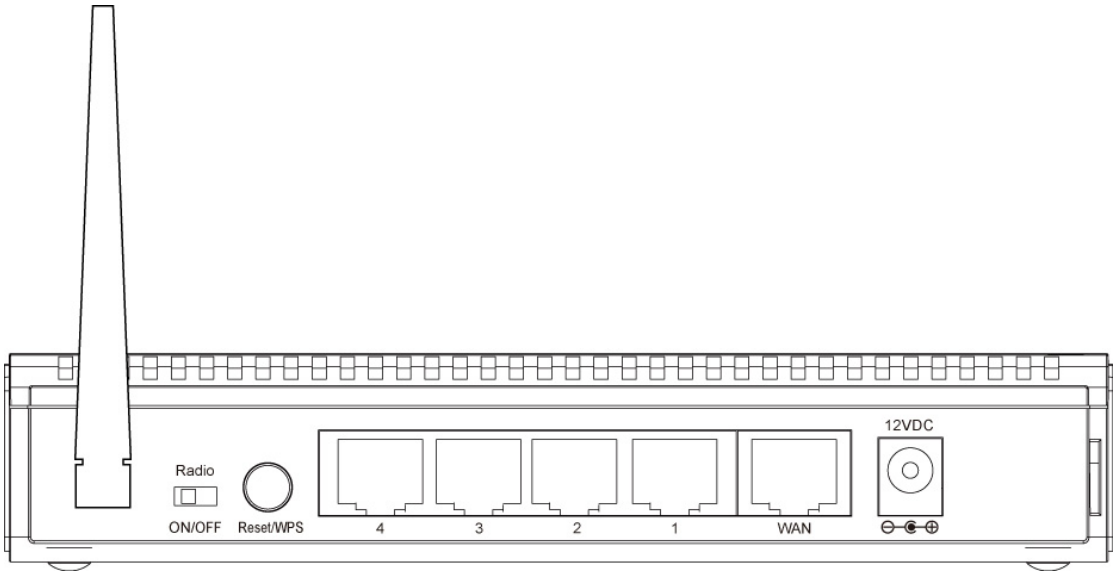
- Wireless 150 Router
- Quick installation guide
- Manual CD
- A/C power adapter
- Ethernet Cable

1.3 Router Interface

Front Panel LEDs

LED	Light Status	Description
POWER	On	Router is powered on.
WLAN	On	WPS setup is in progress.
	Off	Wireless network is switched off.
	Flashing	Wireless network is ready and WPS setup is not in progress.
WAN LNK/ACT	On	WAN port is connected.
	Off	WAN port is not connected.
	Flashing	WAN port is transferring or receiving data.
LAN 1-4 LNK/ACT	On	LAN port is connected.
	Off	LAN port is not connected.
	Flashing	LAN port is transferring or receiving data.

Back Panel



Item Name	Description
Antenna	The antenna is 3dBi dipole antenna.
Radio ON/OFF	Switch the button to activate or deactivate the Router's wireless function.

Reset / WPS	Reset the router to factory default settings (clear all settings) or start security synchronization function (WPS). Press this button and hold for 10 seconds to restore all settings to factory defaults. Press this button for no longer than 1 second to start security synchronization.
1 - 4	Local Area Network (LAN) ports 1 to 4.
WAN	Wide Area Network (WAN / Internet) port.
Power	Power connector, connects to A/C power adapter.

Chapter 2 Connecting the Router

2.1 Building Network Connection

Note: Prior to connecting the router, be sure to power off your computer, DSL/Cable modem(if applicable), and the router.

Step 1 Connect one end of a network cable to the **WAN** port of the router and connect the other end of the cable to the DSL/Cable modem. Power on the modem.

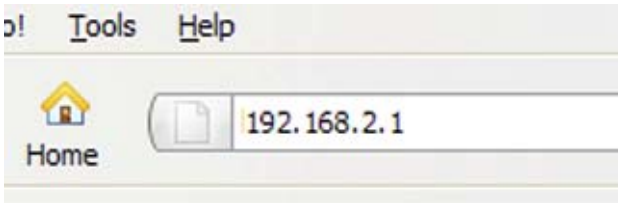
Cable/DSL Modem

Step 2 With another network cable, connect one end of the cable to your computer's Ethernet port and the other end to one of the **LAN** ports on the router. (After setup finishes, you can remove the network cable between the computer and router if you want to use wireless connection.)

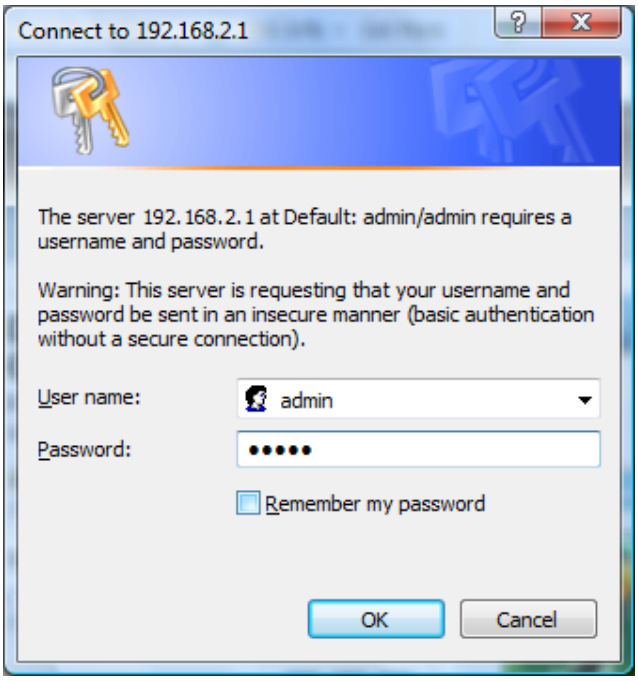
Step 3 Plug the power adapter to the router and connect it to an outlet or power strip.
Step 4 Power on your computer.
Step 5 Make sure **POWER**, **WAN**, **WLAN**, and the **LAN** port that the computer is connected to are lit. If not, try the above steps again.

2.2 Configuring the Router – Setup Wizard

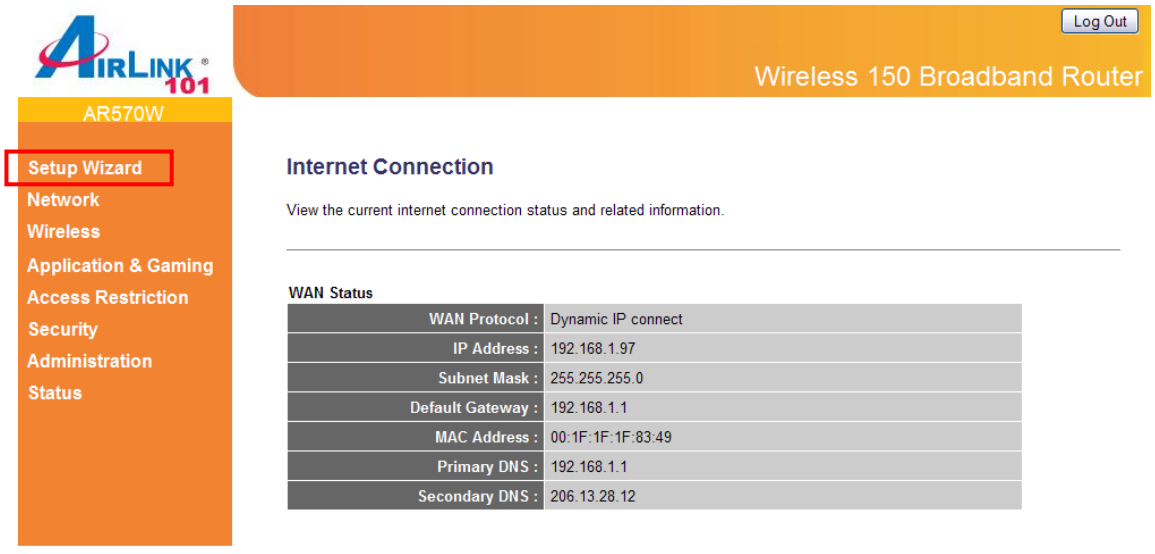
Step 1 Open the web browser (i.e. Internet Explorer or Mozilla Firefox) and type **192.168.2.1** in the URL address bar and press **Enter**.



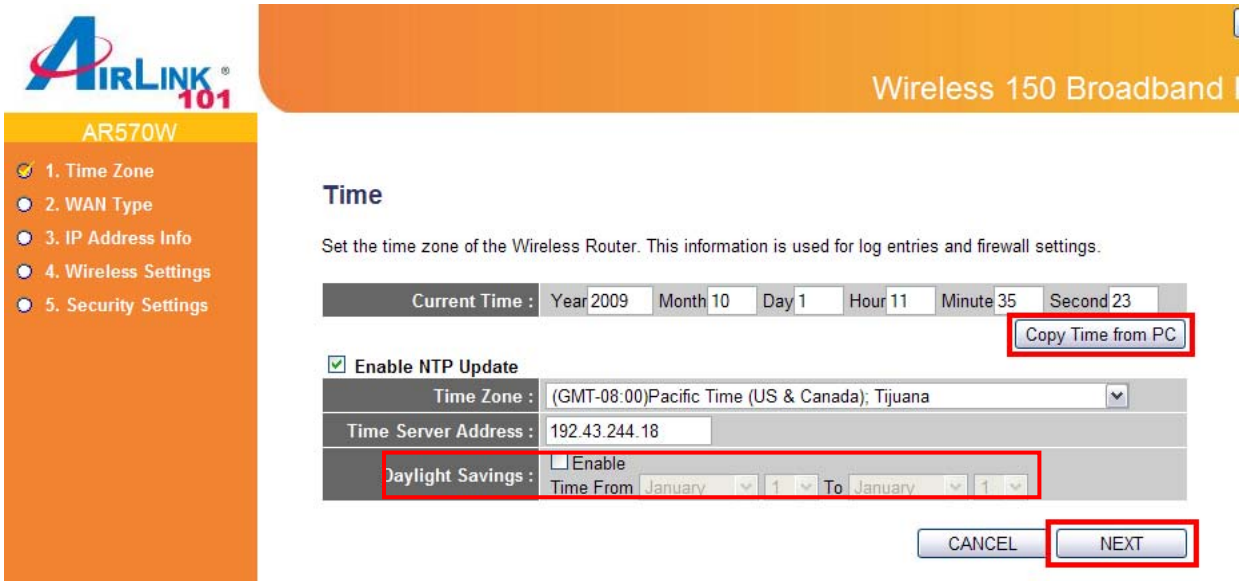
Step 2 Enter **admin** for both the user name and password and click **OK**.


Connect to 192.168.2.1
The server 192.168.2.1 at Default: admin/admin requires a username and password.
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).
User name:
admin
Password:
Remember my password
OK
Cancel

Step 3 Click on Setup Wizard.



Step 4 Configure the Time Zone Settings of the Router. You can click on **Copy Time from PC**. Enable Daylight Saving if it is applicable in your country. Click **NEXT**.



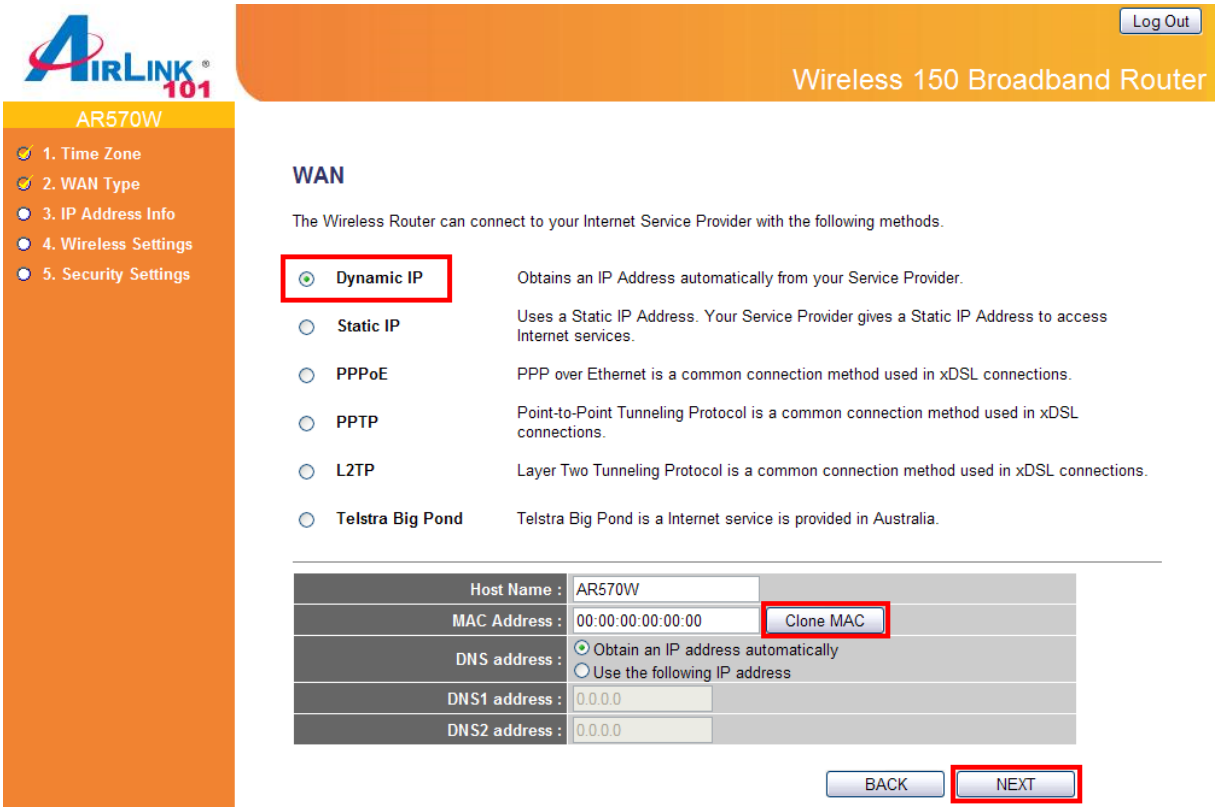
The Time Zone allows your router to base its time on the settings configured here, this will affect functions such as Log entries and Firewall settings.

Parameter	Description
Current Time	Display the router's current time. You can manually configure it or Click on Copy Time from PC.
Enable NTP Update	Check to enable time auto-synchronization through Internet.
Time Zone	You can select your local time zone here. The router will sync time according to your time zone selection.
Time Server Address	Input the IP address / host name of time server here
Daylight Savings	If the country you live uses daylight saving, please check the Enable box and choose the duration of daylight saving.

Step 5 Select WAN type by which Internet service you are using.

Dynamic IP (for Cable or some DSL users)

Click on Dynamic IP if you are connecting to Internet through a cable modem. When the Dynamic IP settings appear below, click **Clone MAC** and click **NEXT**.

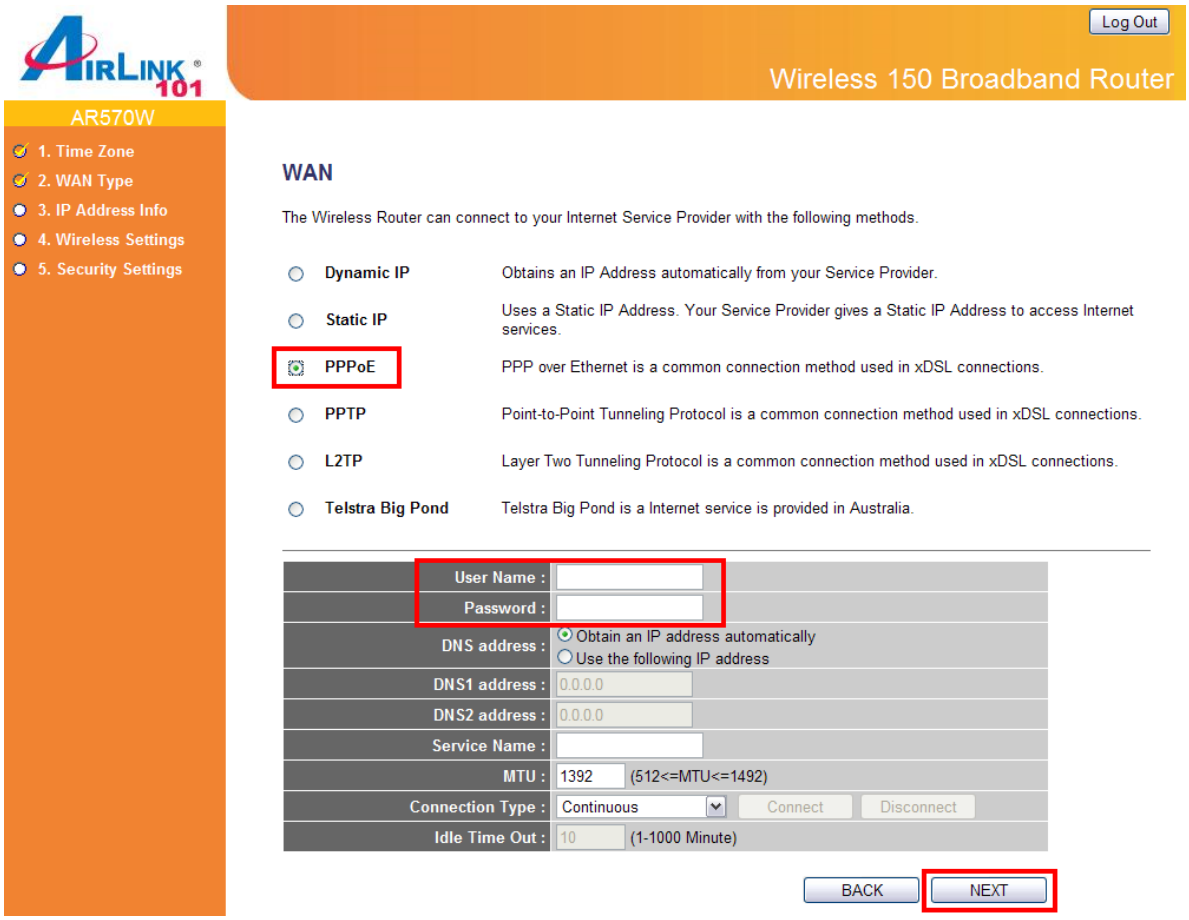

Log Out
Wireless 150 Broadband Router
AR570W
1. Time Zone
2. WAN Type
3. IP Address Info
4. Wireless Settings
5. Security Settings
WAN
The Wireless Router can connect to your Internet Service Provider with the following methods.
Dynamic IP
Obtains an IP Address automatically from your Service Provider.
Static IP
Uses a Static IP Address. Your Service Provider gives a Static IP Address to access Internet services.
PPPoE
PPP over Ethernet is a common connection method used in xDSL connections.
PPTP
Point-to-Point Tunneling Protocol is a common connection method used in xDSL connections.
L2TP
Layer Two Tunneling Protocol is a common connection method used in xDSL connections.
Telstra Big Pond
Telstra Big Pond is a Internet service is provided in Australia.
Host Name :
AR570W
MAC Address :
00:00:00:00:00:00
Clone MAC
DNS address :
Obtain an IP address automatically
Use the following IP address
DNS1 address :
0.0.0.0
DNS2 address :
0.0.0.0
BACK
NEXT

Parameter	Description
Host Name	Please input the host name of your router; this is optional and only required if your service provider asks you to do so.
MAC Address	Please input MAC address of your computer here; if your service provider only permits computer with certain MAC address to access internet. If you are using the computer which used to connect to Internet via cable modem, you can simply press “Clone Mac address” button to fill the MAC address field with the MAC address of your computer.
DNS Address	Select the type of how you obtain IP address from your service provider here. You can choose “Obtain an IP address automatically”, or “Use the following IP address” (i.e. static IP address).
Primary DNS	Please input the IP address of DNS server provided by your service provider.
Secondary DNS	Please input the IP address of another DNS server provided by your service provider, this is optional.

PPPoE (for DSL users)

For DSL users, your Internet type is either **Dynamic IP** or **PPPoE**. If you are not sure which one you have, it is suggested to select **PPPoE** for your WAN type, and if you cannot connect to the Internet after the Setup Wizard finished, go through the Setup Wizard again and **select Dynamic IP**. Otherwise, you can call your ISP to confirm which Internet type you have.

Click on **PPPoE** for your WAN type. Enter your user name and password provided by your ISP. Click **NEXT**.



Note: Depending on the ISP, you may need to include the domain name with your username.

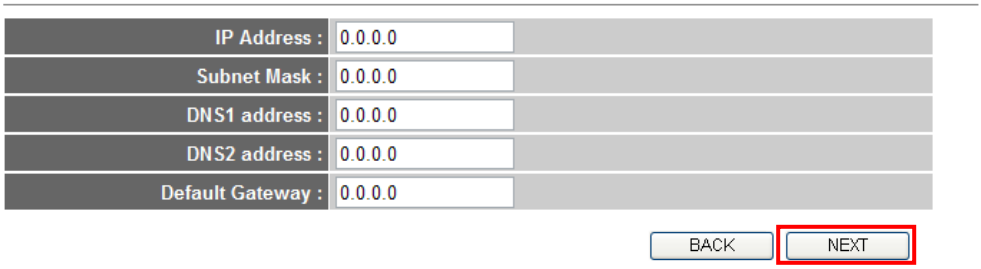
Example: username@sbcglobal.net

Parameter	Description
User Name	Please input user name assigned by your Internet service provider here.
Password	Please input the password assigned by your Internet service provider here.
DNS Address	Select the type of how you obtain IP address from your service provider here. You can choose “Obtain an IP address automatically”, or “Use the following IP address” (i.e. static IP address).
Primary DNS	Please input the IP address of DNS server provided by your service provider.
Secondary DNS	Please input the IP address of another DNS server provided by your service provider, this is optional.

Service Name	Please give a name to this Internet service (this is optional).
MTU	Please input the MTU value of your network connection here. If you don't know, you can use default value.
Connection Type	Please select the connection type you wish to use. There are 3 options: 1) 'Continuous' - keep internet connection alive, do not disconnect, 2) "Connect on Demand" - only connects to Internet when there's a connect attempt. 3) 'Manual' - only connects to Internet when 'Connect' button on this page is pressed, and disconnects when 'Disconnect button is pressed.
Idle Time Out	Specify the time to shutdown internet connect after no internet activity is detected by minute. This option is only available when connection type is 'Connect on Demand'.

Static IP

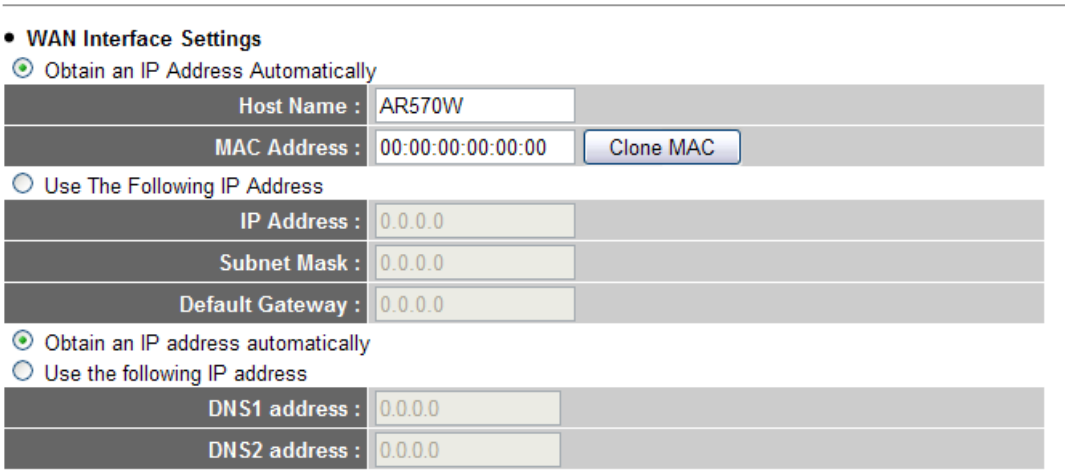
Click on Static IP if your ISP (Internet Service Provider) has provided you a set of IP addresses for your Internet connection.
Enter the IP address, Subnet Mask, DNS addresses and Default Gateway provided by your ISP.
Note: You must use the addresses provided by your Internet service provider, wrong setting value will cause connection problem.



PPTP

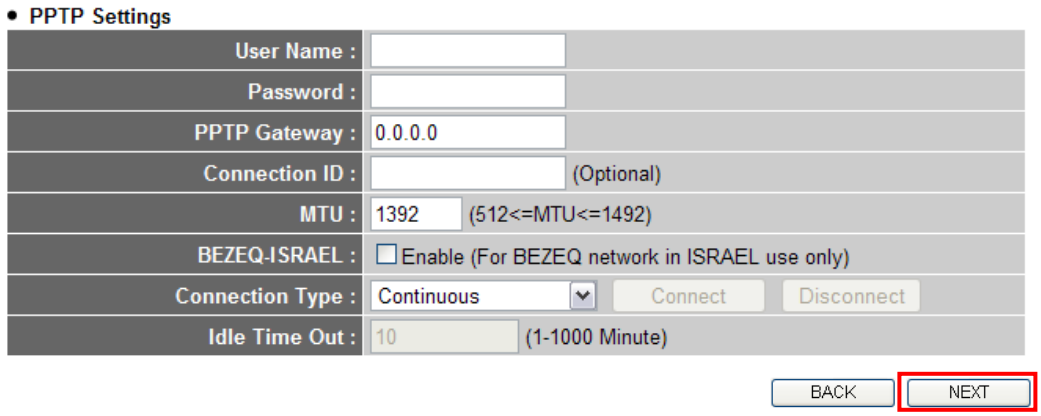
PPTP requires two kinds of setting: WAN interface setting (setup IP address) and PPTP setting (PPTP user name and password).

Here we start from WAN interface setting:



Select the type of how you obtain IP address from your service provider here. You can choose "Obtain an IP address automatically, or "Use the following IP address" (i.e. static IP address) for IP and DNS address. WAN interface settings must be correctly set, or the Internet connection will fail even those settings of PPTP settings are correct. Please contact your Internet service provider if you don't know what you should fill in these fields.

Now please go to PPTP settings section:



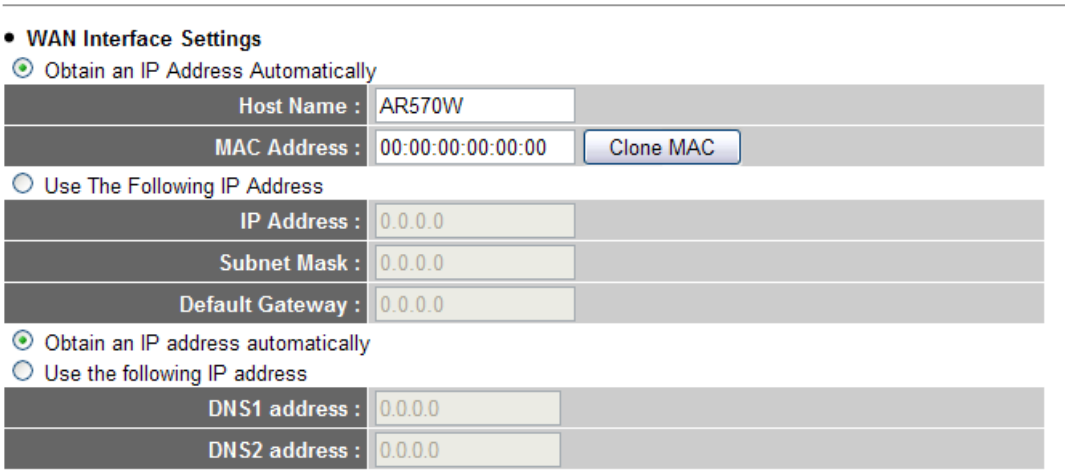
Parameter	Description
User Name	Please input user name assigned by your Internet service provider here.
Password	Please input the password assigned by your Internet service provider here.
PPTP Gateway	Please input the IP address of PPTP gateway assigned by your Internet service provider here.
Connection ID	Please input the connection ID here, this is optional and you can leave it blank.
MTU	Please input the MTU value of your network connection here. If you don't know, you can use default value.
BEZEQ-ISRAEL	Setting item BEZEQ-ISRAEL is only required to check if you're using the service provided by BEZEQ network in Israel.

Connection Type	Please select the connection type of Internet connection you wish to use, please refer to last section for detailed descriptions.
Idle Time Out	Please input the idle time out of Internet connection you wish to use, and refer to last section for detailed descriptions.

When you finish with all settings, please click NEXT.

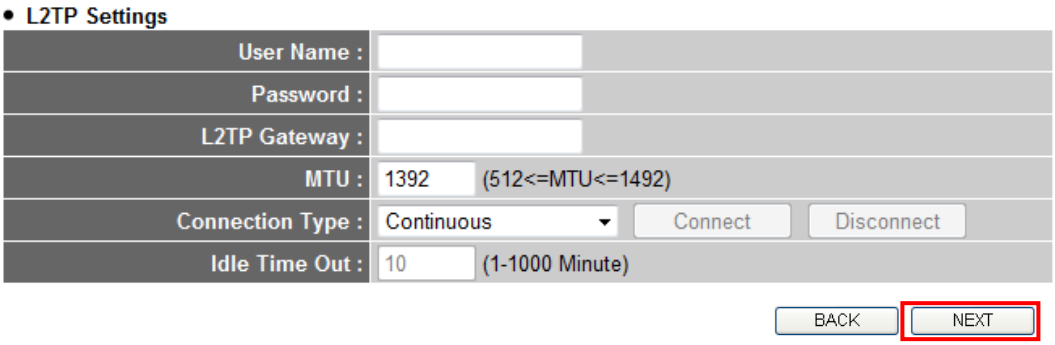
L2TP

L2TP is another connection method for Internet. All required settings are same as PPTP connection. Like PPTP, there are two types of required settings. Start from “WAN Interface Settings”:



Select the type of how you obtain IP address from your service provider here. You can choose “Obtain an IP address automatically, or “Use the following IP address” (i.e. static IP address) for IP and DNS address. WAN interface settings must be correctly set, or the Internet connection will fail even those settings of L2TP settings are correct. Please contact your Internet service provider if you don’t know what you should fill in these fields.

Now please go to L2TP settings section:

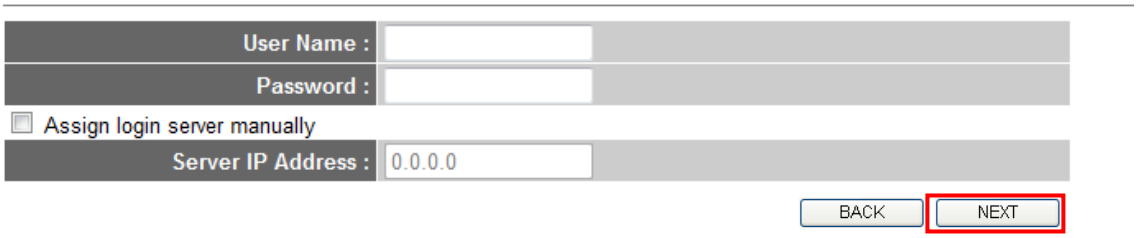


Parameter	Description
User Name	Please input user name assigned by your Internet service provider here.
Password	Please input the password assigned by your Internet service provider here.
L2TP Gateway	Please input the IP address of L2TP gateway assigned by your Internet service provider here.
MTU	Please input the MTU value of your network connection here. If you don't know, you can use default value.
Connection Type	Please select the connection type of Internet connection you wish to use, please refer to last section for detailed descriptions.
Idle Time Out	Please input the idle time out of Internet connection you wish to use, and refer to last section for detailed descriptions.

When you finish with all settings, please click NEXT.

Telstra Big Pond

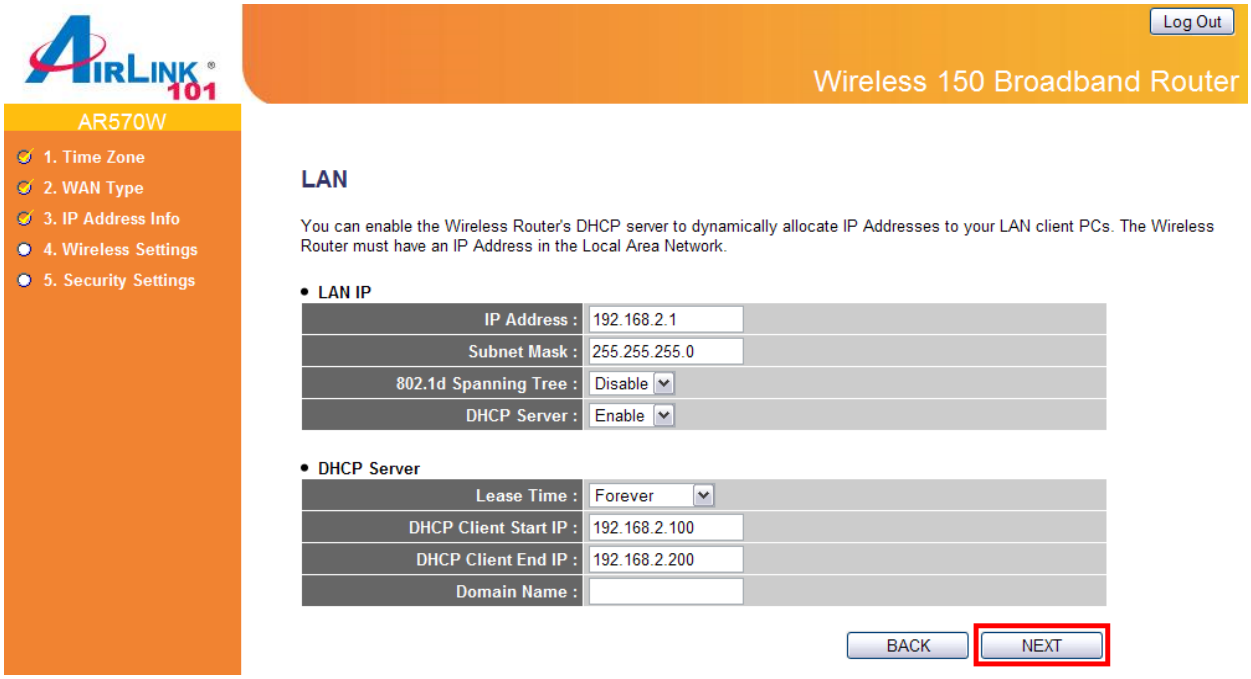
This setting only works when you are using Telstra Big Pond's network service in Australia. You need to input:



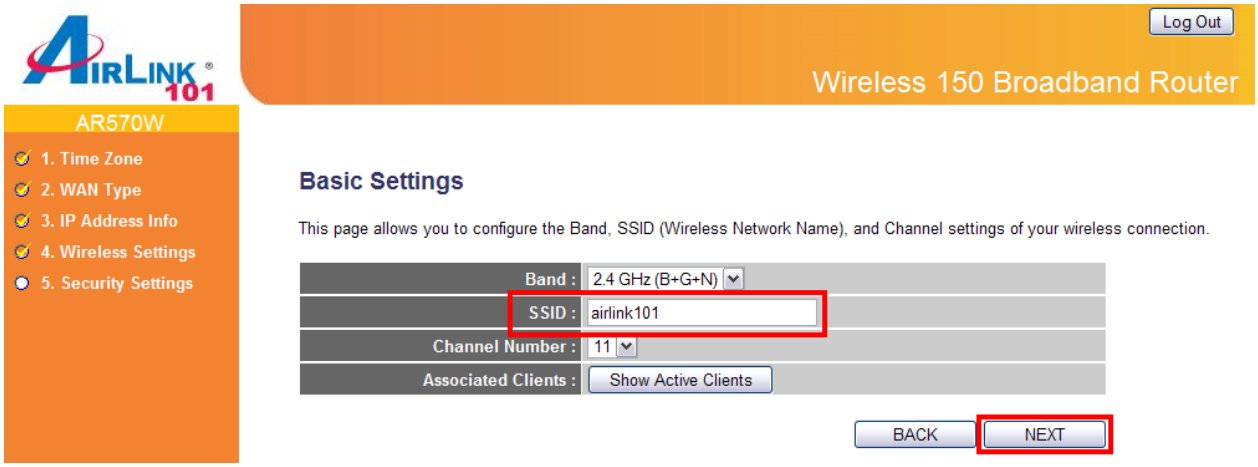
Parameter	Description
User Name	Please input user name assigned by Telstra.
Password	Please input the password assigned by Telstra.
Assign login server manually	Check this box to choose login server by yourself.
Server IP Address	Please input the IP address of login server here.

When you finish with all settings, please click **NEXT**.

Step 6 Keep the default LAN IP and DHCP server settings or modify as needed. Click **NEXT**.


Log Out
Wireless 150 Broadband Router
AR570W
1. Time Zone
2. WAN Type
3. IP Address Info
4. Wireless Settings
5. Security Settings
LAN
You can enable the Wireless Router's DHCP server to dynamically allocate IP Addresses to your LAN client PCs. The Wireless Router must have an IP Address in the Local Area Network.
LAN IP
IP Address : 192.168.2.1
Subnet Mask : 255.255.255.0
802.1d Spanning Tree : Disable
DHCP Server : Enable
DHCP Server
Lease Time : Forever
DHCP Client Start IP : 192.168.2.100
DHCP Client End IP : 192.168.2.200
Domain Name :
BACK
NEXT

Step 7 Keep the default SSID (wireless network name) or change it to a desired name, so you can always recognize your wireless network with it. Click **NEXT**.


Log Out
Wireless 150 Broadband Router
AR570W
1. Time Zone
2. WAN Type
3. IP Address Info
4. Wireless Settings
5. Security Settings
Basic Settings
This page allows you to configure the Band, SSID (Wireless Network Name), and Channel settings of your wireless connection.
Band : 2.4 GHz (B+G+N)
SSID : airlink101
Channel Number : 11
Associated Clients : Show Active Clients
BACK
NEXT

Parameter	Description
Band	Please select the radio band from one of the following options. 2.4GHz (B): 2.4GHz band, only allows 802.11b wireless network client to connect to this router (maximum transfer rate 11Mbps). 2.4 GHz (N): 2.4GHz band, only allows 802.11n wireless network client to connect to this router (maximum transfer rate 150Mbps). 2.4 GHz (B+G):2.4GHz band, only allows 802.11b and 802.11g wireless network client to connect to this router (maximum transfer rate 11Mbps for 802.11b clients, and maximum 54Mbps for 802.11g clients). 2.4 GHz (G): 2.4GHz band, only allows 802.11g wireless network client to connect to this router (maximum transfer rate 54Mbps).

	2.4 GHz (B+G+N): 2.4GHz band, allows 802.11b, 802.11g, and 802.11n wireless network client to connect this router (maximum transfer rate 11Mbps for 802.11b clients, maximum 54Mbps for 802.11g clients, and maximum 150Mbps for 802.11n clients).
SSID	This is the name of the wireless network. You can type any alphanumerical characters here, maximum 32 characters. SSID is used to identify your own wireless router from others when there are multiple wireless routers in the same area. The default SSID is 'airlink101'; it's recommended to change it to a name that you can identify, such as myhome, office_room1, etc.
Channel Number	Select a channel from the dropdown list of 'Channel Number' for broadcasting. You can choose any channel number you want to use, and almost all wireless clients can locate the channel you're using automatically without any problem. However, it's still useful to remember the channel number you use, some wireless client supports manual channel number selecting, and this would help in certain scenario when there is some radio communication problem.
Associated Clients	Click "Show Active Clients" button, then an "Active Wireless Client Table" will pop up. You can see the status of all active wireless stations that are connecting to the access point.

Step 8 Set up Wireless Security for your router.

WPA2(Mixed) is the most secured encryption mode for general users. WEP is the most common encryption but the least secured. It is recommended to use WPA2(Mixed) for your wireless security if all wireless devices on your network support WPA-PSK or WPA2-PSK.

WPA2(Mixed)

Select WPA pre-shared key for Encryption.

Log Out
Wireless 150 Broadband Router
AR570W
1. Time Zone
2. WAN Type
3. IP Address Info
4. Wireless Settings
5. Security Settings
Encryption
This page allows you to set up the wireless security. Configuring encryption for your wireless router can prevent any unauthorized access to your wireless network.
Encryption : WPA pre-shared key
WPA Unicast Cipher Suite : WPA(TKIP) WPA2(AES) WPA2 Mixed
Pre-shared Key Format : Passphrase
Pre-shared Key : ********
Enable 802.1x Authentication
BACK
OK

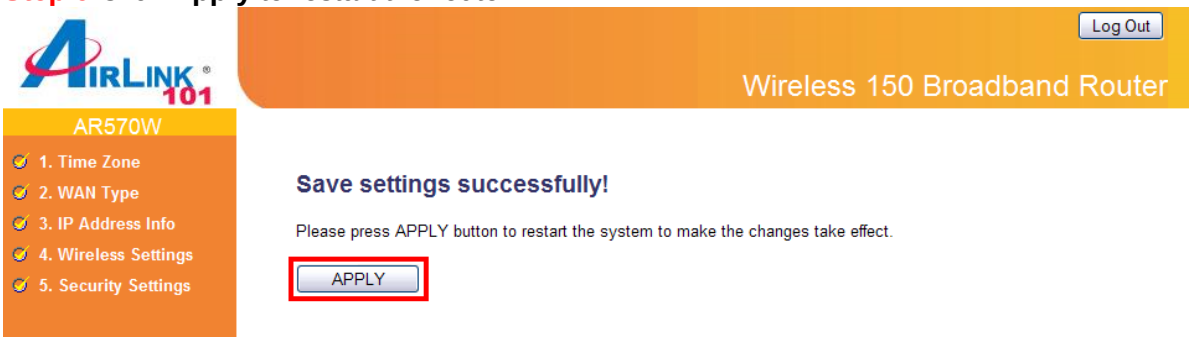
Enter the settings below:

- WPA Unicast Cipher Suite: Select WPA2(Mixed)
- Pre-Shared Key Format: Select Passphrase
- Pre-shared Key: Enter a key between 8 to 63 characters (alphanumeric, case sensitive). This is the security key for your wireless network

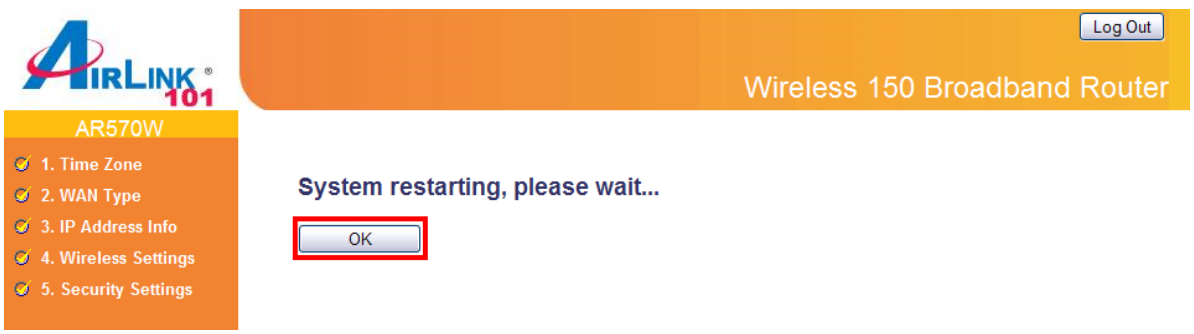
Click **OK** to save the settings.

Note: It is suggested to write down the security settings (Encryption and Key) you configured for the Router on a piece of paper and keep it for you to add more wireless device to your network in the future.

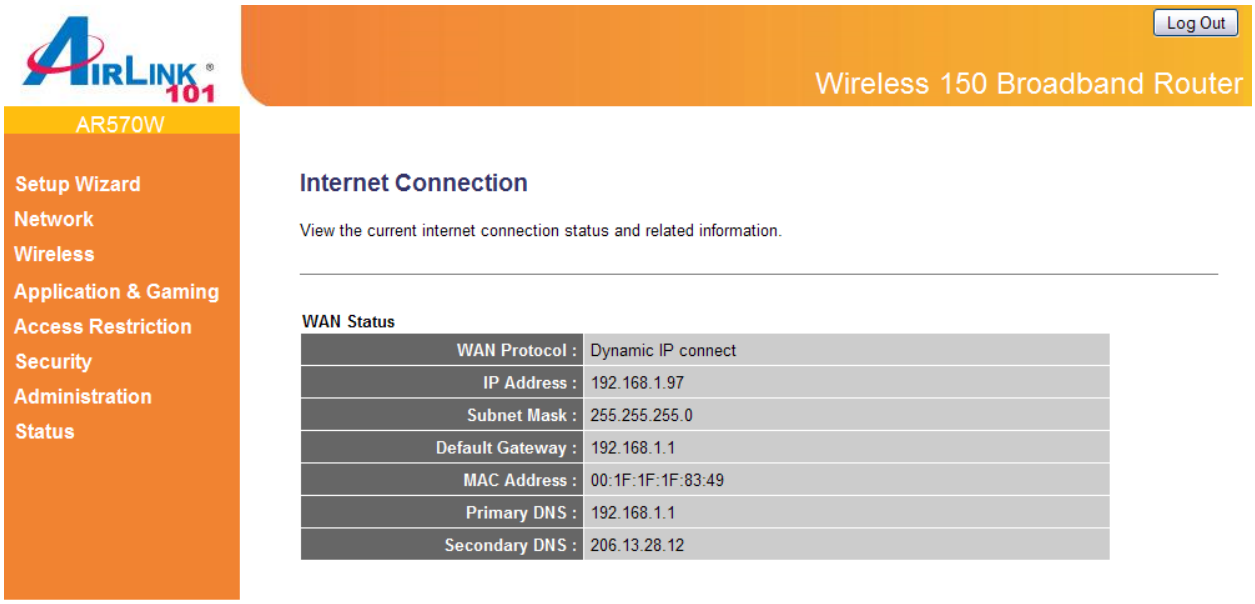
Step 9 Click **Apply** to restart the router.



Step 10 Click **OK**, you will go back to the Status page with valid IP address assigned by you ISP (or configured by yourself if you use Static IP) in WAN Status section.



If each field has valid numbers or IP addresses being assigned, the router is connected to the Internet.



Congratulations! Your router configuration has been finished. You should now be able to access the Internet; if not, please go to Chapter 2.4 for troubleshooting.

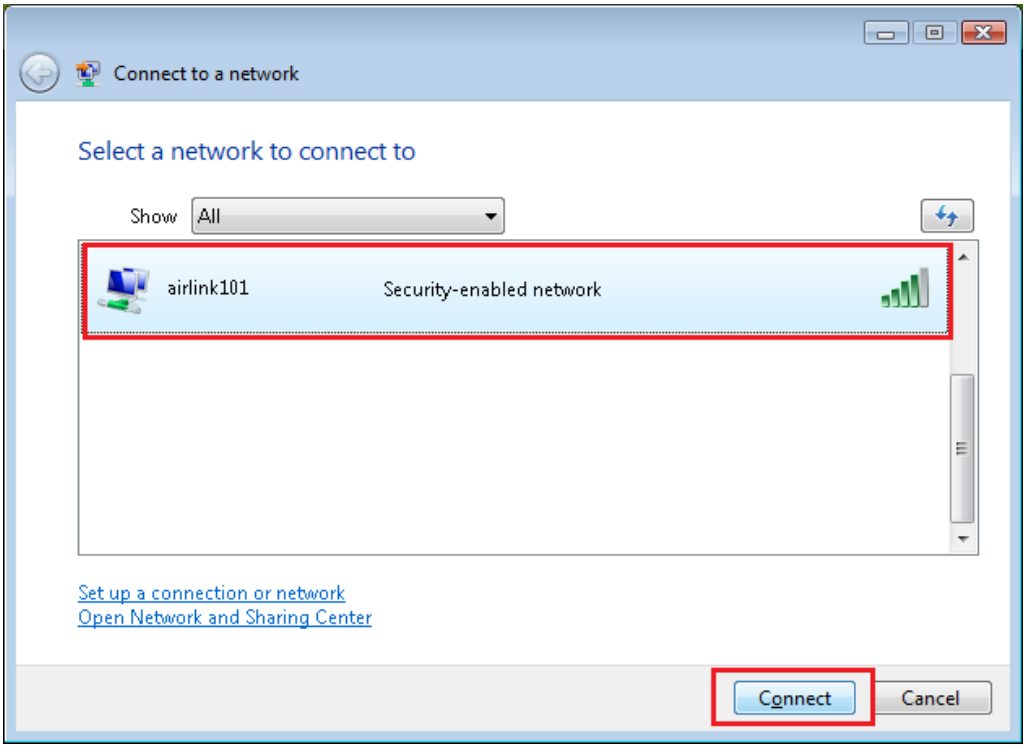
2.3 Connecting to the Router Wirelessly

If you can connect to Internet from your computer that is wired to the Router, you can now set up wireless connection between computer(s) and the Router. If you wish to use wireless on a certain computer, you can now remove the network cable connecting the computer to the router.

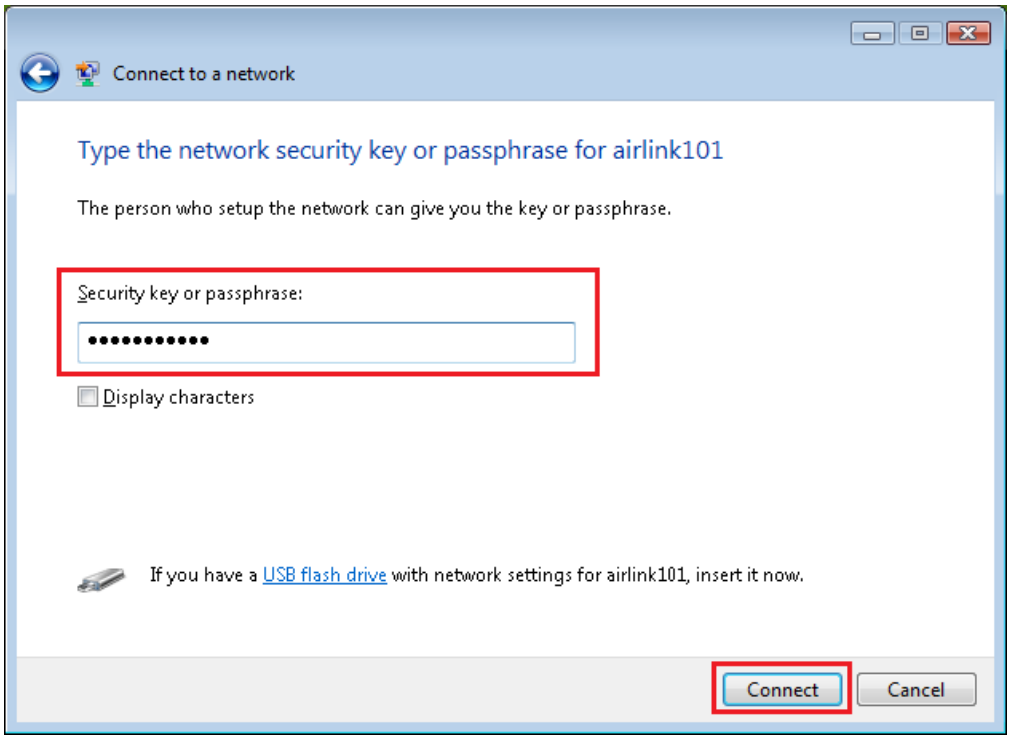
You must configure your wireless computer in order to establish a wireless connection to the router. In this section, you can find the instructions of how to connect to the router wirelessly with your **Vista** computer. You can also refer to the manual of your wireless network card regarding how to connect to a router wirelessly.

Step 1 Click on this icon on the task bar of your desktop, then click on **Wireless networks are available.**

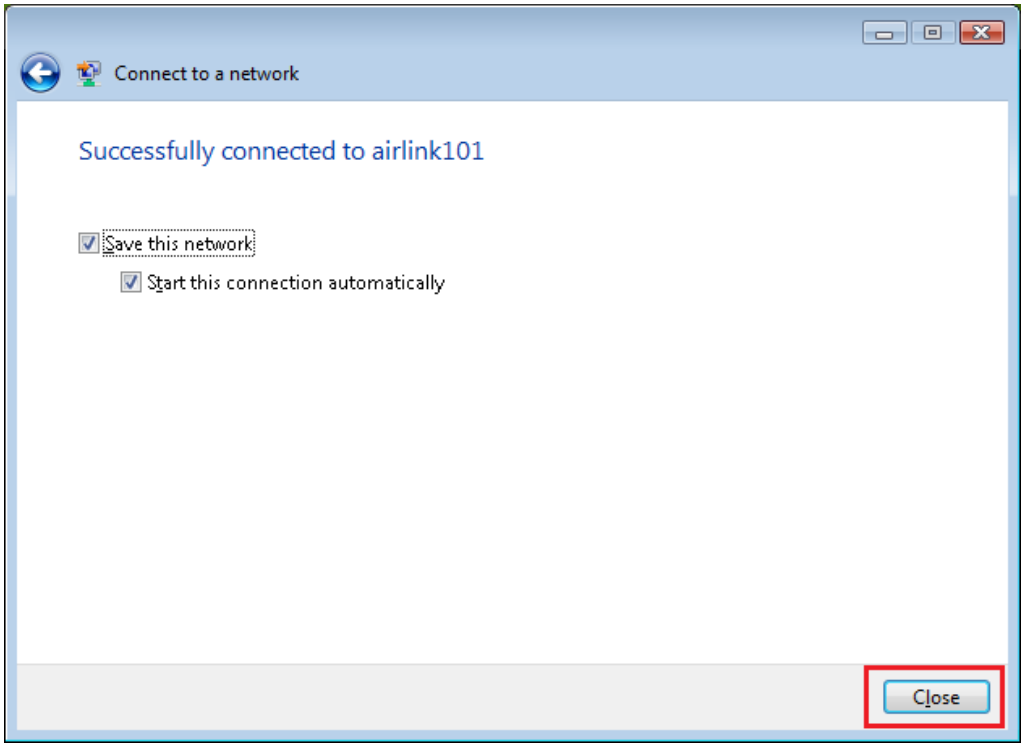
Step 2 Select the wireless network you want to connect to and click **Connect**.



Step 3 Enter the Security key you configured for the Router (see Step 8 in Chapter 2.2). Click **Connect**.


Connect to a network
Type the network security key or passphrase for airlink101
The person who setup the network can give you the key or passphrase.
Security key or passphrase:
Display characters
If you have a USB flash drive with network settings for airlink101, insert it now.
Connect
Cancel

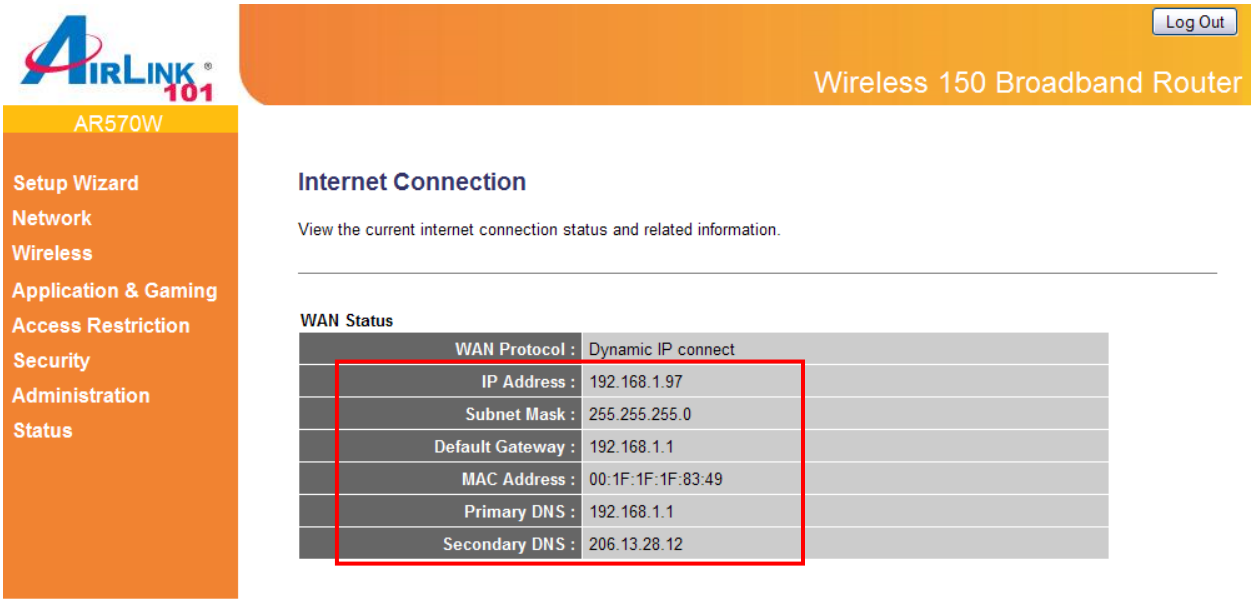
Step 4 Click on **Close**. Now the wireless connection has been established successfully with the Router.



You should be able to connect to Internet wirelessly now.

2.4 Troubleshooting

If you have trouble connecting to the Internet, try the following steps:
Step 1 Power off the Cable/DSL modem, router, and computer and wait for **5 minutes**.
Step 2 Turn on the Cable/DSL modem and wait for the lights on the modem to settle down.
Step 3 Turn on the router and wait for the lights on the router to settle down.
Step 4 Turn on the computer.
Step 5 Log in to the router and you will see the Internet Connection Status.
Step 6 Verify that the **Internet IP Address**, **Subnet Mask**, and **Default Gateway** under **WAN Status** section have valid numbers assigned to them (instead of all 0's).



Chapter 3 Using Web Configuration Utility

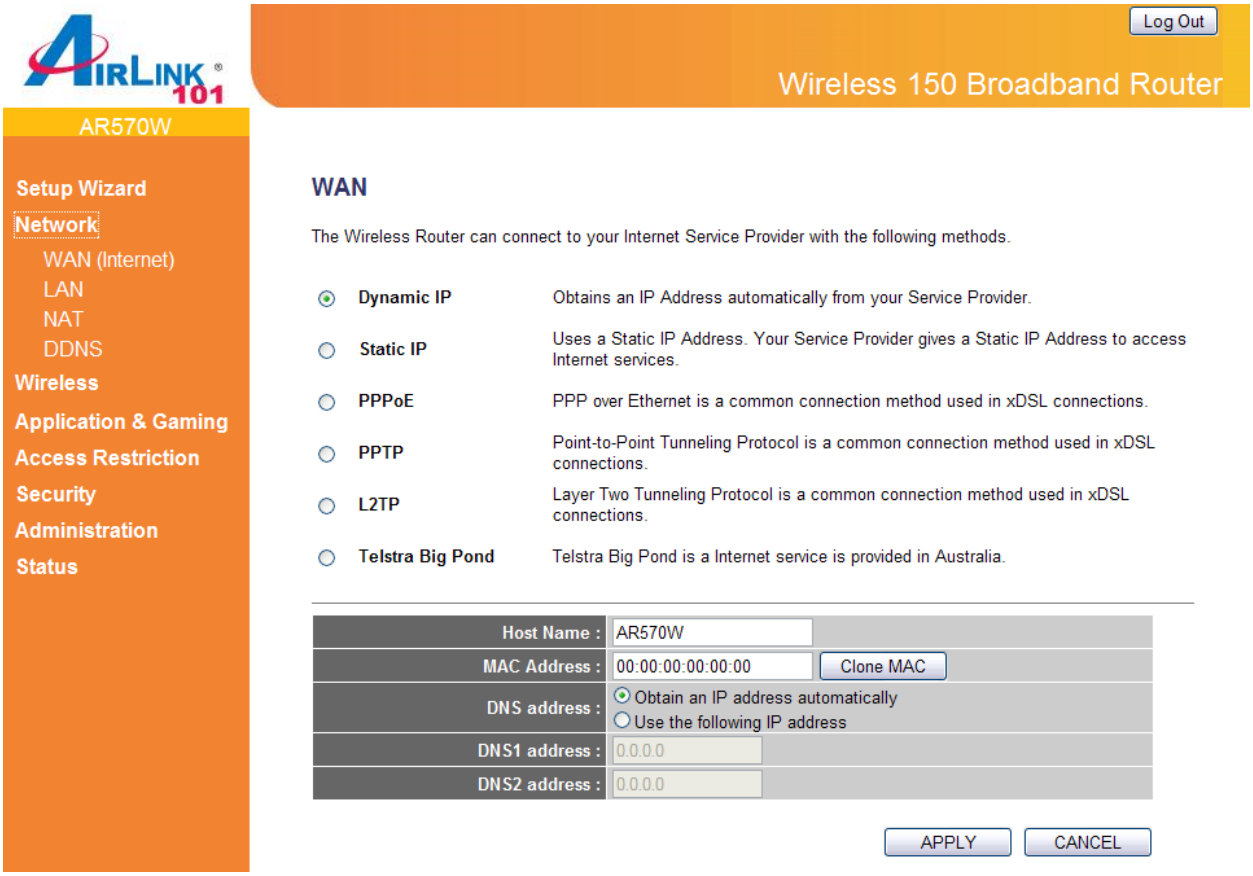
The Web Configuration Utility contains advanced features that allow you to configure the router to meet your network's needs such as: Access Control, QoS (Quality of Service), Port Forwarding (Virtual Server) and other functions. If you have already configured the Setup Wizard, you do NOT need to configure any other thing here for you to start using the Internet. Below is a general description of the advanced functions available for this router.

Menu	Description
3.0 Setup Wizard	This quick setup wizard can guide you through the basic settings of this Router. Please see instructions in Chapter 2.2.
3.1 Network	This section allows you to configure the Internet Connection settings with your ISP, the settings of your local area network (LAN), such as enable/disable the DHCP server, Dynamic DNS information, and NAT function.
3.2 Wireless	This section allows you to setup the Router's SSID, security key, WPS, etc.
3.3 Application & Gaming	This section allows you to configure router's setting for your special applications or gaming requirements, such as open certain ports for your applications.
3.4 Access Restrictions	This section allows you to set up the access control rules, such as MAC filtering, URL filtering to prevent the LAN users from accessing certain type of website.
3.5 Security	This Firewall section allows you to configure Hacker Prevention and VPN pass through.
3.6 Administration	The section allows you to specify a time zone, change the system password, save/reload the router configuration, upgrade firmware and so on.
3.7 Status	You can see Router's status in this section.

3.1 Network

3.1.1 WAN

Use the WAN setting page to change your Internet connection type. The WAN setting page allows you to configure the Internet connection type of your ISP. The WAN settings offer the following selections for the router's WAN port, **Dynamic IP, Static IP, PPPoE**, **PPTP**, **L2TP** and **Telstra Big Pond**. Please choose one type and complete the detail settings below.



Please see **Chapter 2.2**, **Step 5** for the detailed description of each WAN type.

3.1.2 LAN

This page allows you to specify an IP address for your router, configure the DHCP Server and Static DHCP Lease Table.

➢ LAN IP section

Parameters	Default	Description
IP address	192.168.2.1	This is the router's LAN IP address (Your LAN clients' default gateway IP address).
Subnet Mask	255.255.255.0	Specify a Subnet Mask for your LAN segment.
802.1d Spanning Tree	Disable	If you wish to activate 802.1d spanning tree function, select "Enabled", or set it to "Disabled" If 802.1d Spanning Tree function is enabled, this router will use the spanning tree protocol to prevent from network loop happened in the LAN ports.
DHCP Server	Enable	By enablting the DHCP server, the router will automatically give your LAN clients an IP address. If the DHCP server is not enabled then you'll have to manually set your LAN client's IP addresses; make sure the LAN Client is in the same subnet as this broadband router if you want the router to be your LAN client's default gateway.

➢ DHCP Server section

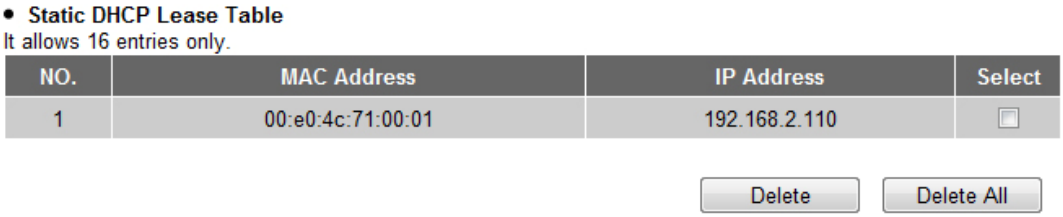
Parameters	Description
Lease Time	Please choose a lease time (the duration that every computer can keep a specific IP address) of every IP address assigned by this router from dropdown menu.
DHCP Client Start IP	Please input the start IP address of the IP range.
DHCP Client End IP	Please input the end IP address of the IP range.
Domain Name	If you wish, you can also optionally input the domain name for your network. This is optional.

➢ Static DHCP Lease Table section

This function allows you to assign a static IP address to a specific computer forever, so you don't have to manually set the IP address for a computer, and still enjoy the benefit of using DHCP server. Maximum 16 static IP addresses can be assigned here. (If you set "Lease Time" to forever in **DHCP Server** section, you can assign an IP address to a specific computer permanently).

Parameters	Description
Enable Static DHCP Leases	Check this box to enable this function, otherwise DHCP uncheck it to disable this function.
MAC Address	Input the MAC address of the computer or network device (total 12 characters, with character from 0 to 9, and from a to f, like "00:11:22:aa:bb:cc")
IP address	Input the IP address you want to assign to this computer or network device
Add	After you entered MAC address and IP address pair, click this button to add the pair to static DHCP leases table.

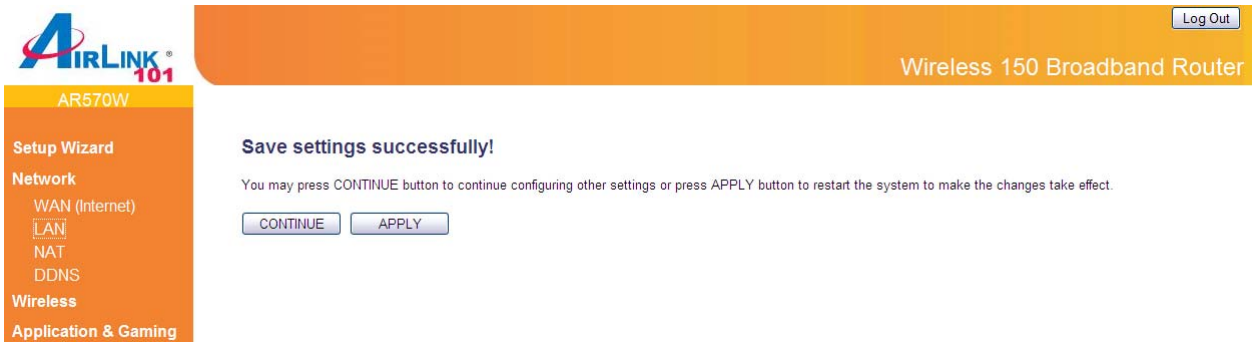
After you clicked "Add", the MAC address and IP address mapping will be added to "Static DHCP Lease Table" section.



If you want to delete a specific item, please check the “Select” box of a MAC address and IP address mapping, then click “Delete” button. If you want to delete all mappings, click “Delete All”.

After you finish with all settings, please click “Apply” button.
If you want to reset all settings in this page, please click “Cancel” button.

After you clicked Apply, the following message will be displayed on your web browser:



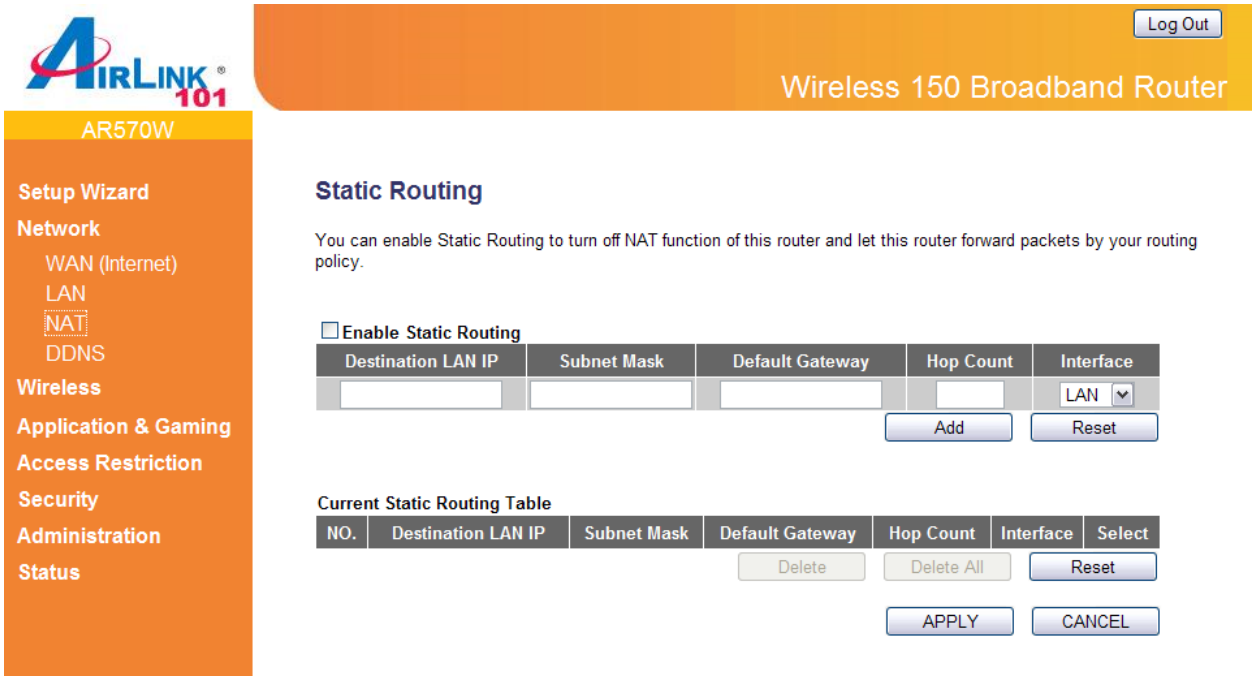
You can click “Continue” to back to previous setup page to continue on other setup procedures, or click “Apply” to reboot the router so the settings will take effect (Please wait for about 30 seconds while router is rebooting).

3.1.3 NAT / Static Routing

Network address translations (NAT) shares a single public IP address to multiple computers. All computers must be assigned a valid public IP address to be able to get connected to Internet, but Internet service providers provide very few public IP addresses to each user based on service plans, usually 1 for each household. Therefore, it’s necessary to use NAT technology to share a single Internet IP address to multiple computers on a same local network, so everyone can get connected to Internet.

The NAT function is enabled by default; to disable it, you need to enable Static Routing by checking the “Enable Static Routing” box. Do not disable NAT unless you have professional knowledge on routing.

Please follow the following instructions to set Static Routing parameters:



Parameter	Description
Enable Static Routing	Check/uncheck to disable/enable the NAT function.
Destination LAN IP	Enter the IP Address of the destination LAN.
Subnet Mask	Enter the Subnet Mask of the destination LAN.
Default Gateway	This is the gateway IP Address where packets are sent. Input the gateway IP Address.
Hop Count	Enter the maximum number of steps between network nodes that data packets will travel. A node is any device on the network, such as a computer, print server, or router.
Interface	This interface tells you whether the Destination IP Address is on the **LAN & Wireless** (Ethernet and wireless networks) or the **WAN** (Internet).
Add	Click on Add to add the routing rule to Router's routing table.
Reset	You can also click 'Reset' button to clear all data you entered.

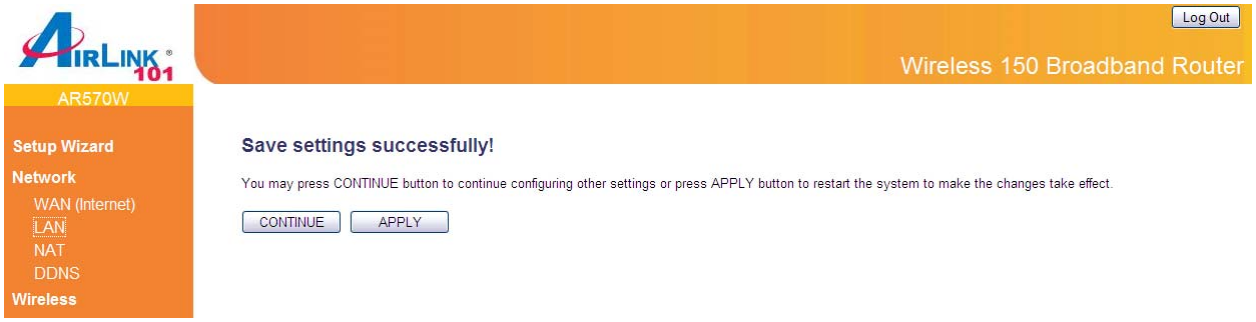
From the **Current Static Routing Table**, you can check each Static Routing setting.

Parameter	Description
Delete	If you want to delete a setting, check the 'select' box of the setting you want to delete, then click 'Delete' button. (You can select more than one setting).
Delete All	If you want to delete all settings listed here, please click 'Delete All' button.

Reset	You can also click 'Reset' button unselect all.

After you finish with all settings, please click "Apply" button.
If you want to reset all settings in this page, please click "Cancel" button.

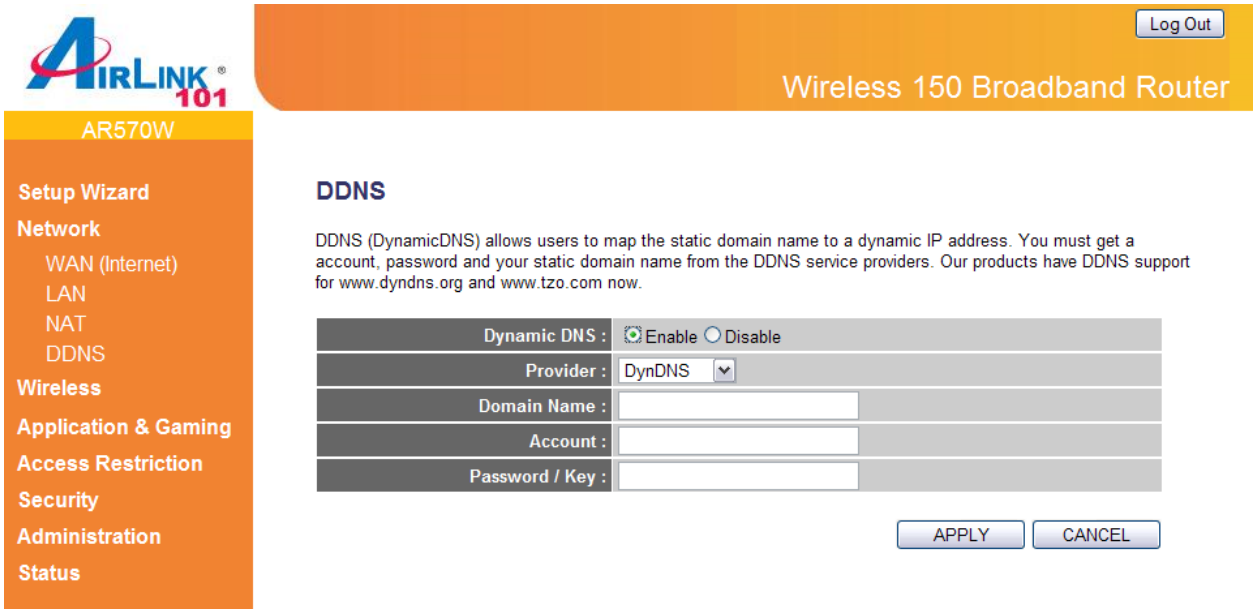
After you clicked Apply, the following message will be displayed on your web browser:



You can click "Continue" to back to previous setup page to continue on other setup procedures, or click "Apply" to reboot the router so the settings will take effect (Please wait for about 30 seconds while router is rebooting).

3.1.4 DDNS

DDNS allows you to map the static domain name to a dynamic IP address. You must get an account, password and a static domain name from a DDNS service provider. This router supports DynDNS (www.dyndns.org), and TZO (www.tzo.com).

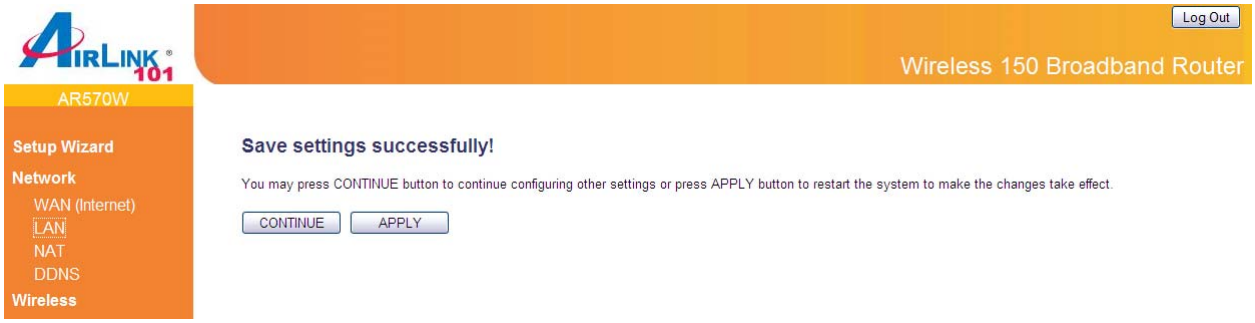


Parameters	Default	Description
Dynamic DNS	Disable	Enable/Disable the DDNS function of this router.

Provider	Select a DDNS service provider.
Domain name	Your static domain name that use DDNS.
Account	The account/username that your DDNS service provider assigned to you.
Password/Key	The password you set for the DDNS service account above.

After you finish with all settings, please click “Apply” button.
If you want to reset all settings in this page, please click “Cancel” button.

After you clicked Apply, the following message will be displayed on your web browser:

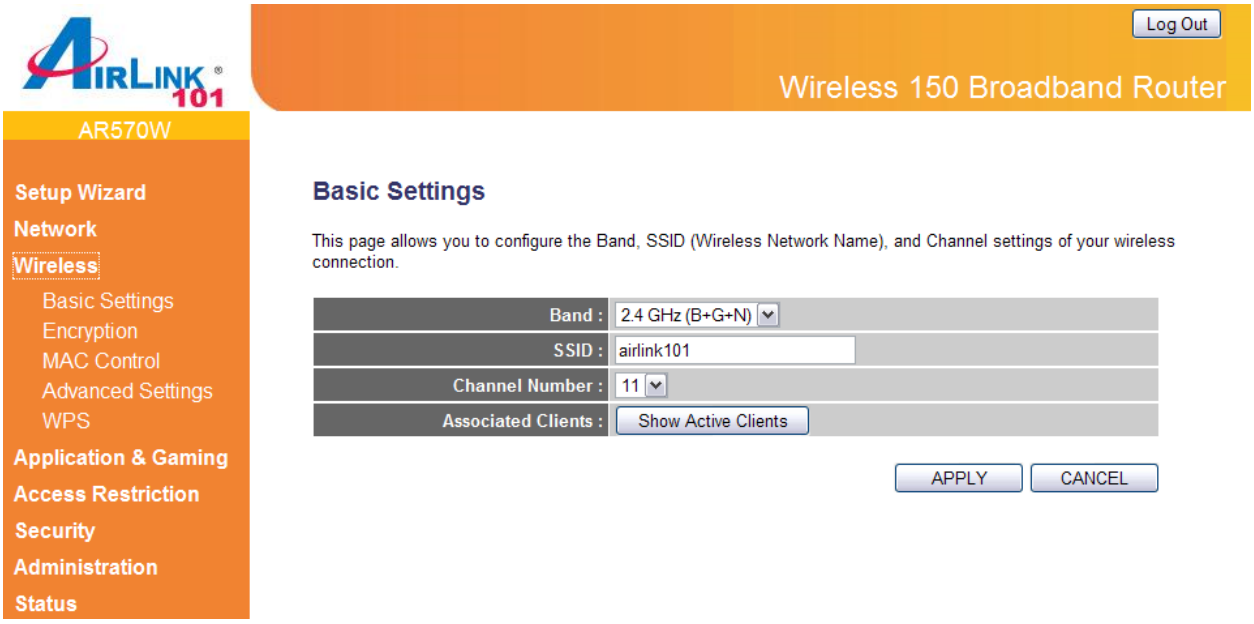


You can click “Continue” to back to previous setup page to continue on other setup procedures, or click “Apply” to reboot the router so the settings will take effect (Please wait for about 30 seconds while router is rebooting).

3.2 Wireless

3.2.1 Basic Settings

You can set parameters that are used for wireless clients to connect to this router. The parameters include SSID, Channel Number, etc.

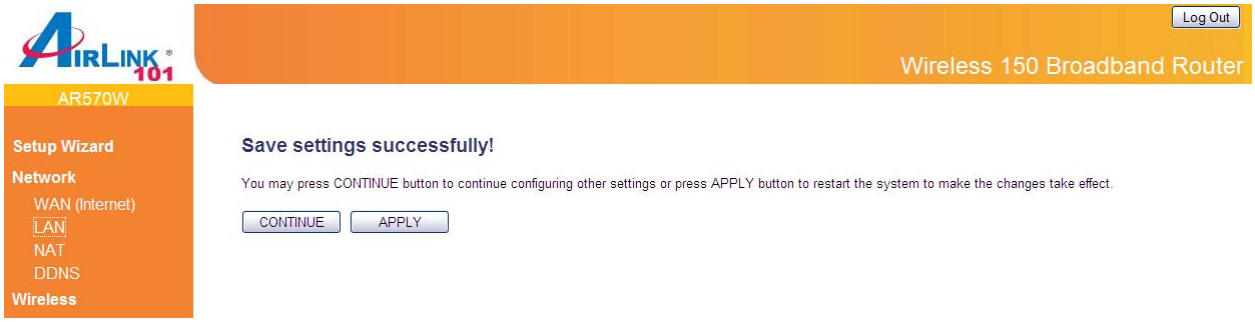


Parameters	Default	Description
Band	2.4 GHz (B+G+N)	Please select the radio band from one of the following options. 2.4GHz(B): 2.4GHz band, only allows 802.11b wireless network client to connect this router (maximum transfer rate 11Mbps*). 2.4 GHz (N): 2.4GHz band, only allows 802.11n wireless network client to connect this router (maximum transfer rate 150Mbps*). 2.4 GHz (B+G):2.4GHz band, only allows 802.11b and 802.11g wireless network client to connect this router (maximum transfer rate 11Mbps for 802.11b clients, and maximum 54Mbps for 802.11g clients*). 2.4 GHz (G): 2.4GHz band, only allows 802.11g wireless network client to connect this router (maximum transfer rate 54Mbps*). 2.4 GHz (B+G+N): 2.4GHz band, allows 802.11b, 802.11g, and 802.11n wireless network client to connect this router (maximum transfer rate 11Mbps for 802.11b clients, maximum 54Mbps for 802.11g clients, and maximum 150Mbps for 802.11n clients*).

SSID	airlink101	This is the name of your wireless network. You can type any alphanumerical characters here, maximum 32 characters. SSID is used to identify your own wireless router from others when there are other wireless routers in the same area. It's recommended to change default SSID value to the one which is meaningful to you, like myhome, office_room1, etc.
Channel Number	6	Please select a channel from the dropdown list of 'Channel Number' for broadcasting. You can choose any channel number you want to use, and almost all wireless clients can locate the channel you're using automatically without any problem. However, it's still useful to remember the channel number you use, some wireless client supports manual channel number select, and this would help in certain scenario when there is some radio communication problem.
Show Active Clients		Click "Show Active Clients" button, then an "Active Wireless Client Table" will pop up. You can see the status of all active wireless clients that are connecting to the Router.

After you finish with all settings, please click "Apply" button.
If you want to reset all settings in this page, please click "Cancel" button.

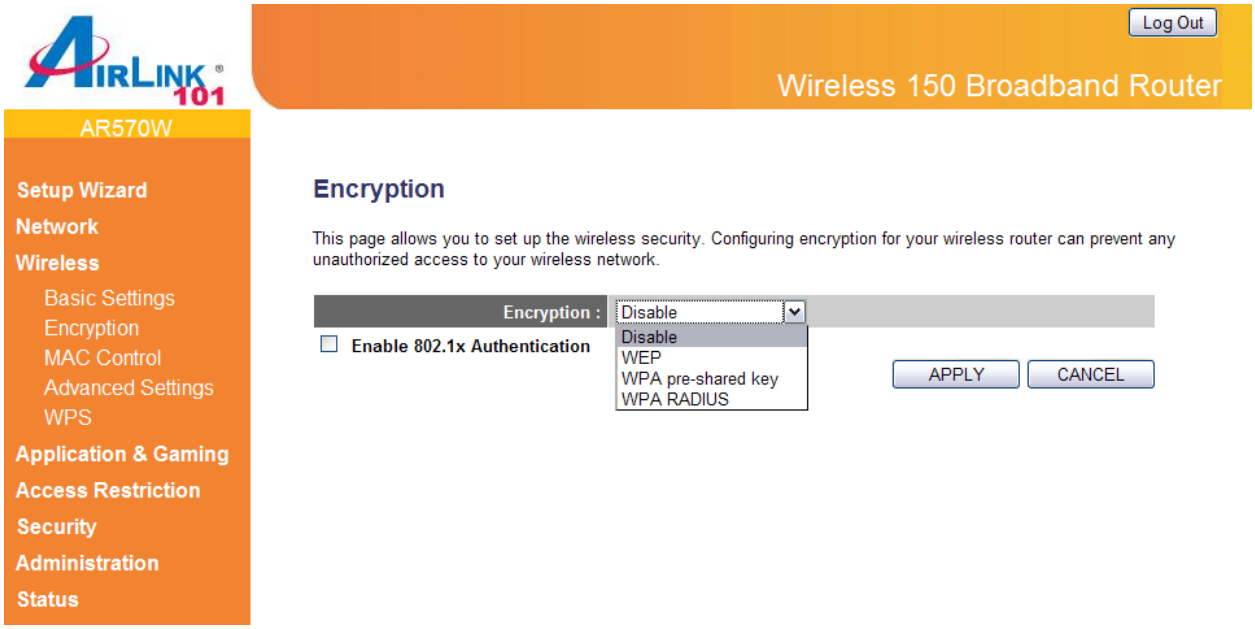
After you clicked Apply, the following message will be displayed on your web browser:



You can click "Continue" to back to previous setup page to continue on other setup procedures, or click "Apply" to reboot the router so the settings will take effect (Please wait for about 30 seconds while router is rebooting).

3.2.2 Wireless Security

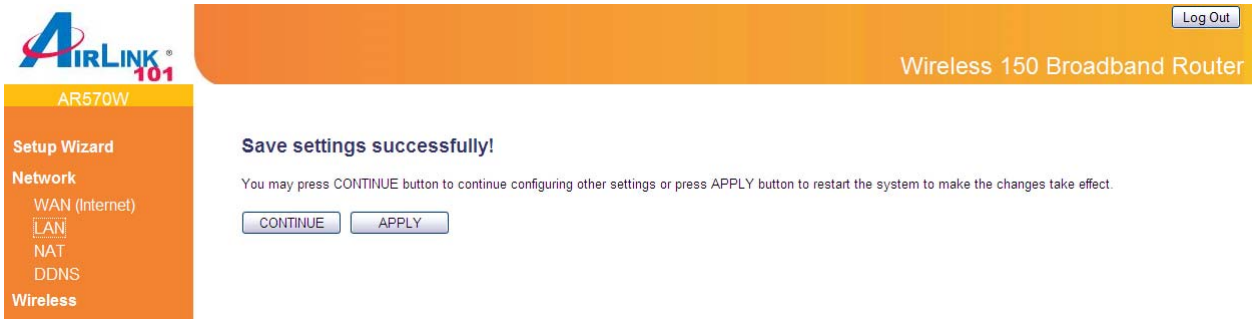
The AR570W Wireless 150 Router provides complete wireless LAN security functions, including WEP, IEEE 802.11x, WPA2/WPA-PSK and WPA with RADIUS. With these security functions, you can prevent your wireless LAN from illegal access. Please make sure your wireless clients use the same security settings.



Parameters	Default	Description
Encryption		You can choose Disable, WEP, WPA pre-share key, WPA RADIUS for encryption mode. The detailed settings will appear after you choose an encryption. **See 3.2.2.1 to 3.2.2.3 for each encryption type.**
Enable 802.1x Authentication		IEEE 802.1x is an authentication protocol. Every user must use a valid account to login to this Access Point before accessing the wireless LAN. The authentication is processed by a RADIUS server. Check this box to authenticates user by IEEE 802.1x.

After you finish with all security settings, please click “Apply” button.
If you want to reset all settings in this page, please click “Cancel” button.

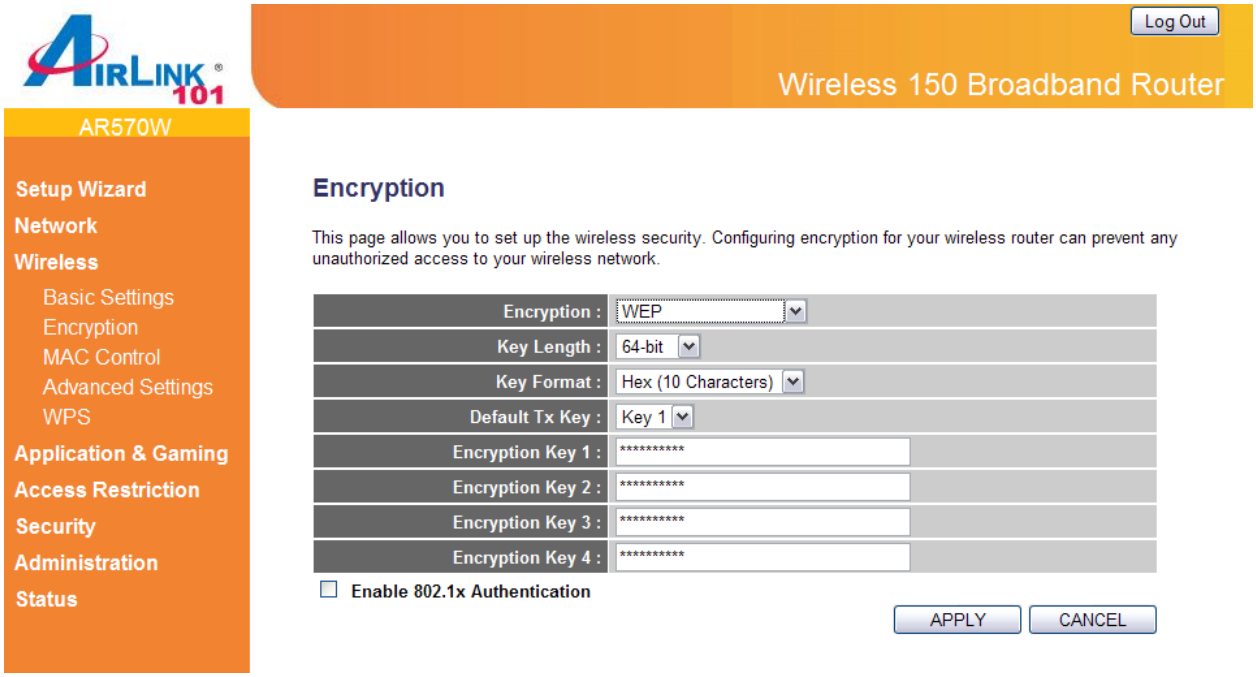
After you clicked Apply, the following message will be displayed on your web browser:



You can click “Continue” to back to previous setup page to continue on other setup procedures, or click “Apply” to reboot the router so the settings will take effect (Please wait for about 30 seconds while router is rebooting).

3.2.2.1 WEP

Select “WEP” for the “Encryption” mode if you wish to use WEP to encrypt your wireless network.

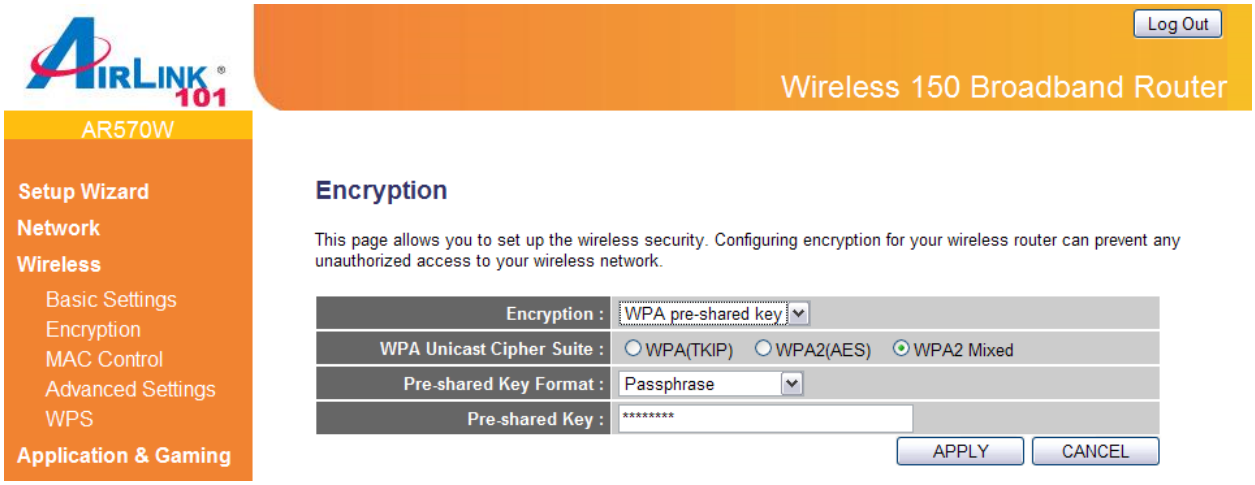


Parameters	Description
Key Length	You can select the WEP key length for encryption, 64-bit or 128-bit. Larger WEP key length will provide higher level of security, but the throughput will be lower.
Key Format	You may select to select ASCII Characters (alphanumeric format) or Hexadecimal Digits (in the “A-F”, “a-f” and “0-9” range) to be the WEP Key.
Default Tx Key	You can set up to four sets of WEP key, and you can decide which key is being used by default here. If you don’t know which one you should use, select ‘Key 1’.
Encryption Key 1~4	The WEP key are used to encrypt data transmitted in the wireless network. Fill the text box by following the rules below. 64-bit WEP: input 10-digit Hex values (in the “A-F”, “a-f” and “0-9” range) or 5-digit ASCII character as the encryption keys. 128-bit WEP: input 26-digit Hex values (in the “A-F”, “a-f” and “0-9” range) or 13-digit ASCII characters as the encryption keys.

3.2.2.2 WPA Pre-share Key

Wi-Fi Protected Access (WPA) is an advanced security standard. You can use a pre-shared key to authenticate wireless stations and encrypt data during communication. It uses TKIP/AES to

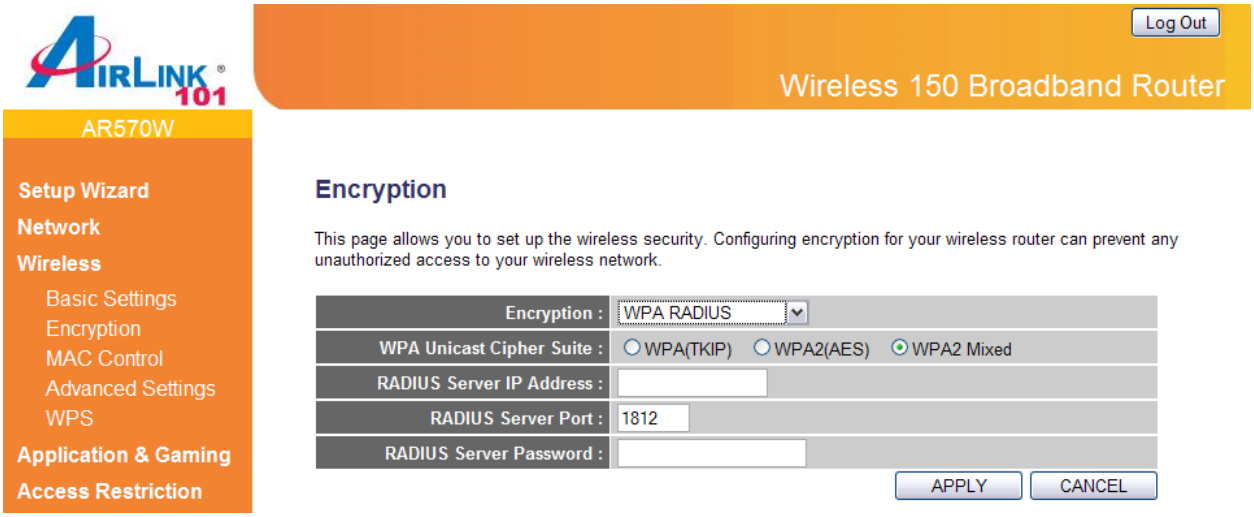
change the encryption key frequently. So the encryption key is not easy to be broken by hackers. This can improve security very much.
Select “WPA Pre-share Key” for the “Encryption” mode if you wish to use WPA-PSK or WPA2-PSK to encrypt your wireless network.



Parameters	Description
WPA Unicast Cipher Suite	Available options are: WPA (TKIP), WPA2 (AES), and WPA2 Mixed. WPA2 (Mixed) support both WPA-PSK(TKIP/AES) and WPA2-PSK(TKIP/AES). Please make sure your wireless client supports the cipher you selected.
Pre-shared Key Format	You may select Passphrase (alphanumeric format) or Hex (in the “A-F”, “a-f” and “0-9” range) to be the Pre-shared Key.
Pre-shared Key	The Pre-shared key is used to authenticate and encrypt data transmitted in the wireless network. You may create your own key here for wireless clients to connect to your router.

3.2.2.3 WPA RADIUS

IEEE 802.1x is an authentication protocol. Every user must use a valid account to login to this wireless router before accessing the wireless LAN. The authentication is processed by a RADIUS server. This mode only authenticates user by IEEE 802.1x, but it does not encryption the data during communication.
Select “WPA RADIUS” for the “Encryption” mode if you wish to use WPA RADIUS to encrypt your wireless network.

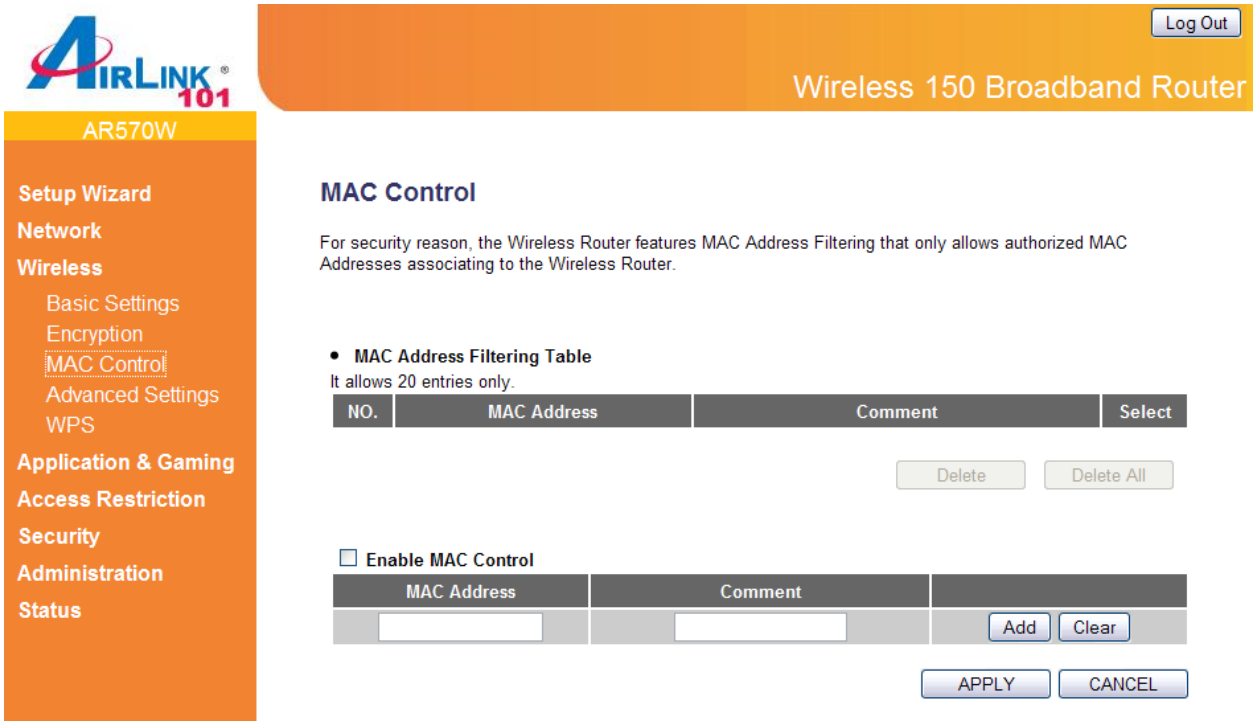


Parameters	Description
WPA Unicast Cipher Suite	Please select a type of WPA cipher suite. Available options are: WPA (TKIP), WPA2 (AES), and WPA2 Mixed. You can select one of them, but you have to make sure your wireless client support the cipher you selected.
RADIUS Server IP Address	Please input the IP address of your Radius authentication server here.
RADIUS Server Port	Please input the port number of your Radius authentication server here. Default setting is 1812.
RADIUS Server Password	Please input the password of your Radius authentication server here.

3.2.3 MAC Control

This function will help you to prevent unauthorized users from connecting to your wireless router. Only those wireless devices with the MAC addresses you specified here are allowed to access your wireless router. You can use this function with other security measures described in previous section together to enhance the safety of your wireless network.

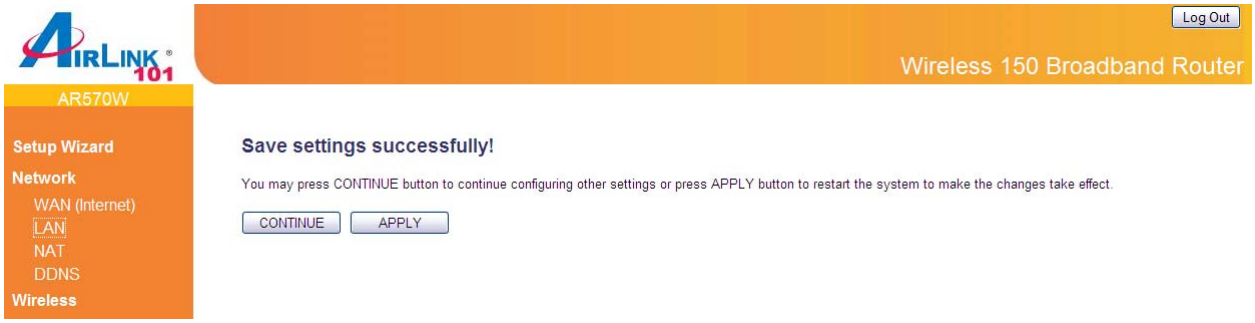
Up to 20 MAC addresses can be added by using this function.



Parameters	Description
Enable MAC Control	Check/Uncheck to enable/disable wireless MAC control.
MAC Address	Input the MAC address of your wireless devices here, format 'xx:xx:xx:xx:xx:xx'.
Comment	You can input any text here as the comment of this MAC address, like 'ROOM 2A Computer' or anything.
Add	Click "Add" button to add the MAC address and associated comment to the MAC address filtering table.
Clear	Click "Clear" to remove the value you inputted in MAC address and comment field.
Delete	If you want to delete a specific MAC address entry, check the 'select' box of the MAC address you want to delete, then click 'Delete' button. (You can select more than one MAC addresses).
Delete All	If you want to delete all MAC addresses listed here, please click 'Delete All' button.

After you finish with all settings, please click "Apply" button.
If you want to reset all settings in this page, please click "Cancel" button.

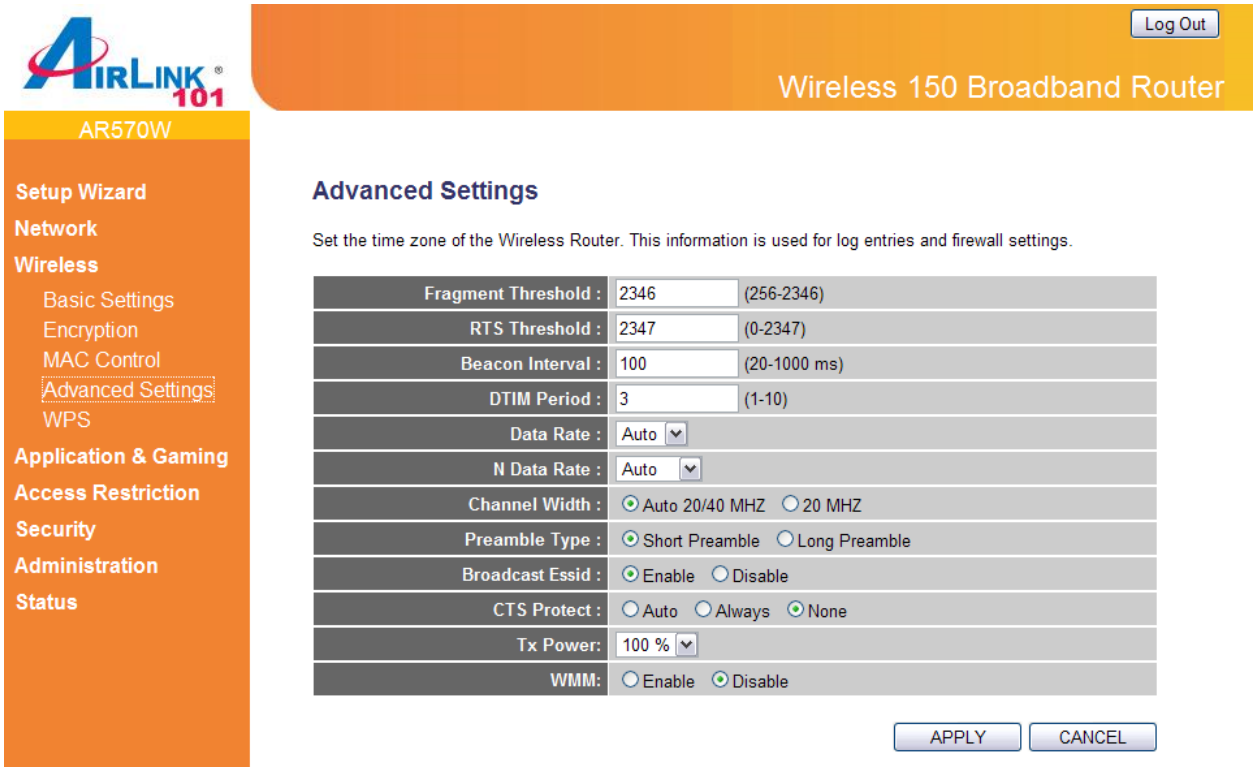
After you clicked Apply, the following message will be displayed on your web browser:



You can click “Continue” to back to previous setup page to continue on other setup procedures, or click “Apply” to reboot the router so the settings will take effect (Please wait for about 30 seconds while router is rebooting).

3.2.4 Advanced Settings

You can set advanced wireless LAN parameters of this router. The parameters include Authentication Type, Fragment Threshold, RTS Threshold, Beacon Interval, Preamble Type, etc. It is suggested not to change these parameters unless you know what effect the changes will have on this router.

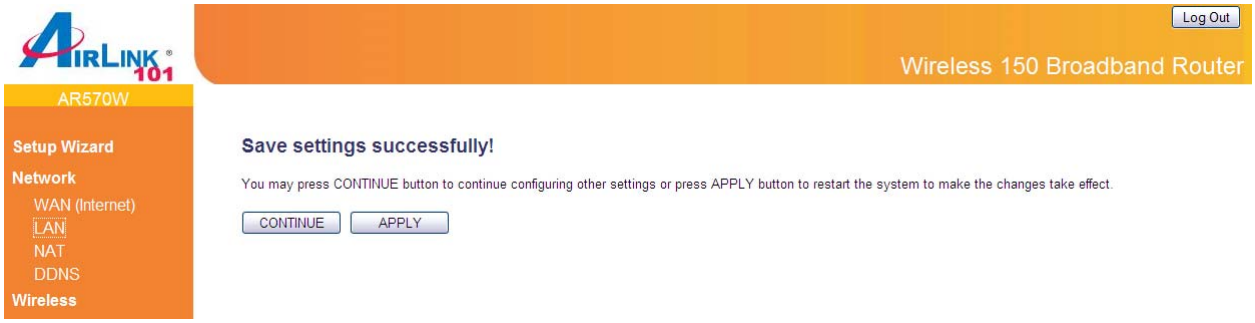


Parameters	Description
Fragment Threshold	“Fragment Threshold” specifies the maximum size of packet during the fragmentation of data to be transmitted. The default value is 2346.

RTS Threshold	When the packet size is smaller than the RTS threshold, the wireless router will not use the RTS/CTS mechanism to send this packet.
Beacon Interval	The interval of time that this wireless router broadcast a beacon. Beacon is used to synchronize the wireless network.
DTIM Period	Set the DTIM period of wireless radio. Do not modify default value if you don't know what it is, default value is 3.
Data Rate	Set the wireless data transfer rate to a certain value. Since most of wireless devices will negotiate with each other and pick a proper data transfer rate automatically, it's not necessary to change this value unless you know what will happen after modification.
N Data Rate	Same as above, but only for 802.11n clients.
Channel Width	Set channel width of wireless radio. Do not modify default value if you don't know what it is, default setting is 'Auto 20/40 MHz'.
Preamble Type	The "Long Preamble" can provide better wireless LAN compatibility while the "Short Preamble" can provide better wireless LAN performance.
Broadcast ESSID	Decide if the wireless router will broadcast its own ESSID or not. You can hide the ESSID of your wireless router by selecting "Disable"
CTS Protect	It is recommended to enable the protection mechanism. This mechanism can decrease the rate of data collision between 802.11b and 802.11g/802.11n wireless stations. When the protection mode is enabled, the throughput of the AP will be a little lower due to many of frame traffic should be transmitted.
Tx Power	You can set the output power of wireless radio. Unless you are using this wireless router in a really big space, you may not have to set output power to 100%. This will enhance security (malicious / unknown users in distance will not be able to reach your wireless router).
WMM	The short of Wi-Fi MultiMedia, it will enhance the data transfer performance of multimedia contents when they are being transferred over wireless network. The default value is "Disable".

After you finish with all settings, please click "Apply" button.
If you want to reset all settings in this page, please click "Cancel" button.

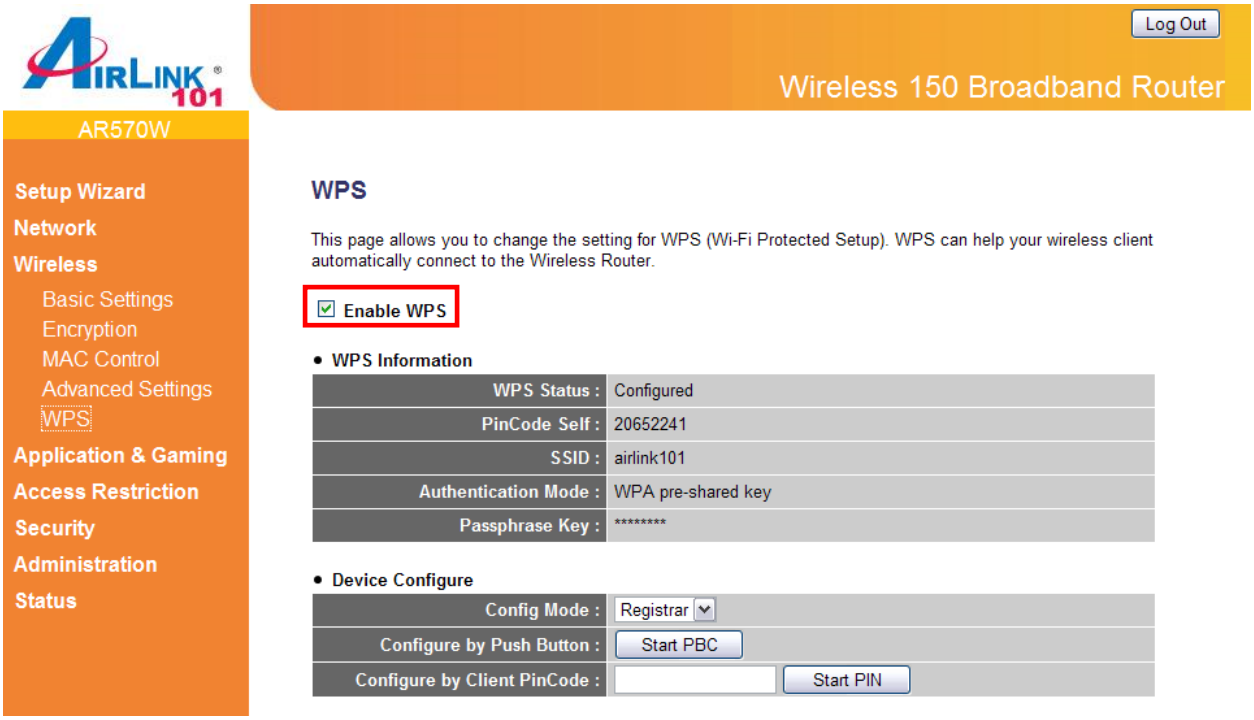
After you clicked Apply, the following message will be displayed on your web browser:



You can click “Continue” to back to previous setup page to continue on other setup procedures, or click “Apply” to reboot the router so the settings will take effect (Please wait for about 30 seconds while router is rebooting).

3.2.5 WPS

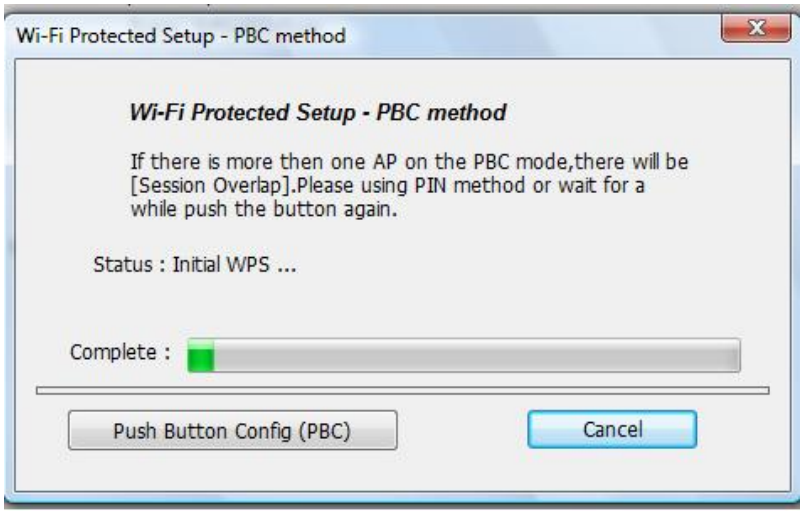
The Airlink101 Wireless 150 Router AR570W has a built-in Easy Setup Button which allows you to connect your wireless computer with the router easily and safely. Your wireless adapter must support this feature as well. If not, you will need to set up the wireless security manually and you can skip this section.



Please make sure this feature is enabled on the Router (see the screenshot above). In the instructions below, we are going to use the Airlink101 WLAN Monitor utility comes with the AWLL6077 Airlink101 Wireless N USB Adapter as an example.

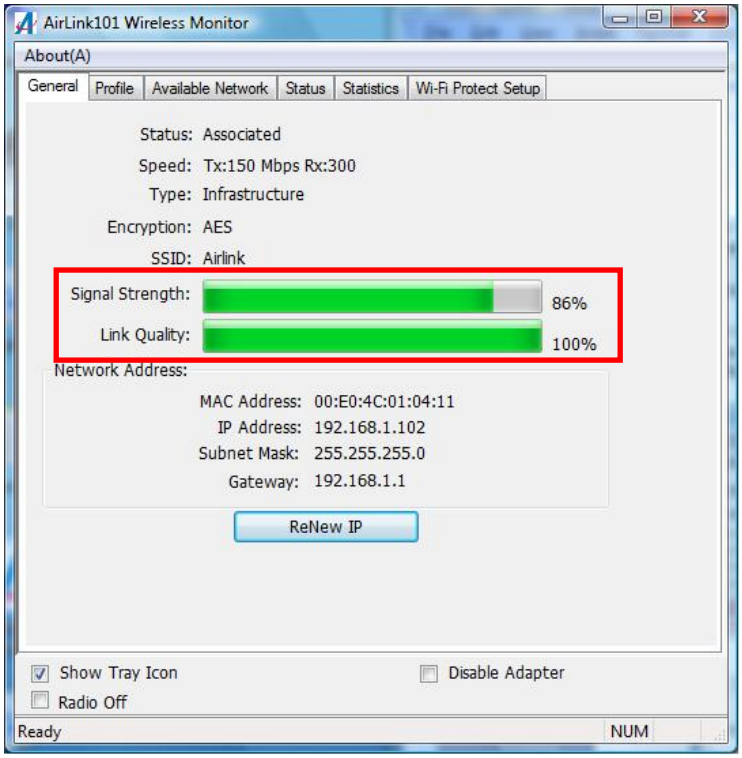
Step 1 Go to the computer with Airlink101 Wireless N USB adapter, AWLL6077 connected.

Step 2 Push and hold the Easy Setup Button on the Adapter until you see the following window pops up on the computer monitor.


Wi-Fi Protected Setup - PBC method
Wi-Fi Protected Setup - PBC method
If there is more then one AP on the PBC mode,there will be [Session Overlap].Please using PIN method or wait for a while push the button again.
Status : Initial WPS ...
Complete :
Push Button Config (PBC)
Cancel

Step 3 Within the following 2 minutes, push the Easy Setup Button the Router. The WLAN LED will stay solid green instead of blinking.

Step 4 The Router will now start the handshake with the wireless adapter which will take about 30 seconds. When you see the window similar to the one below, the connection has been established.



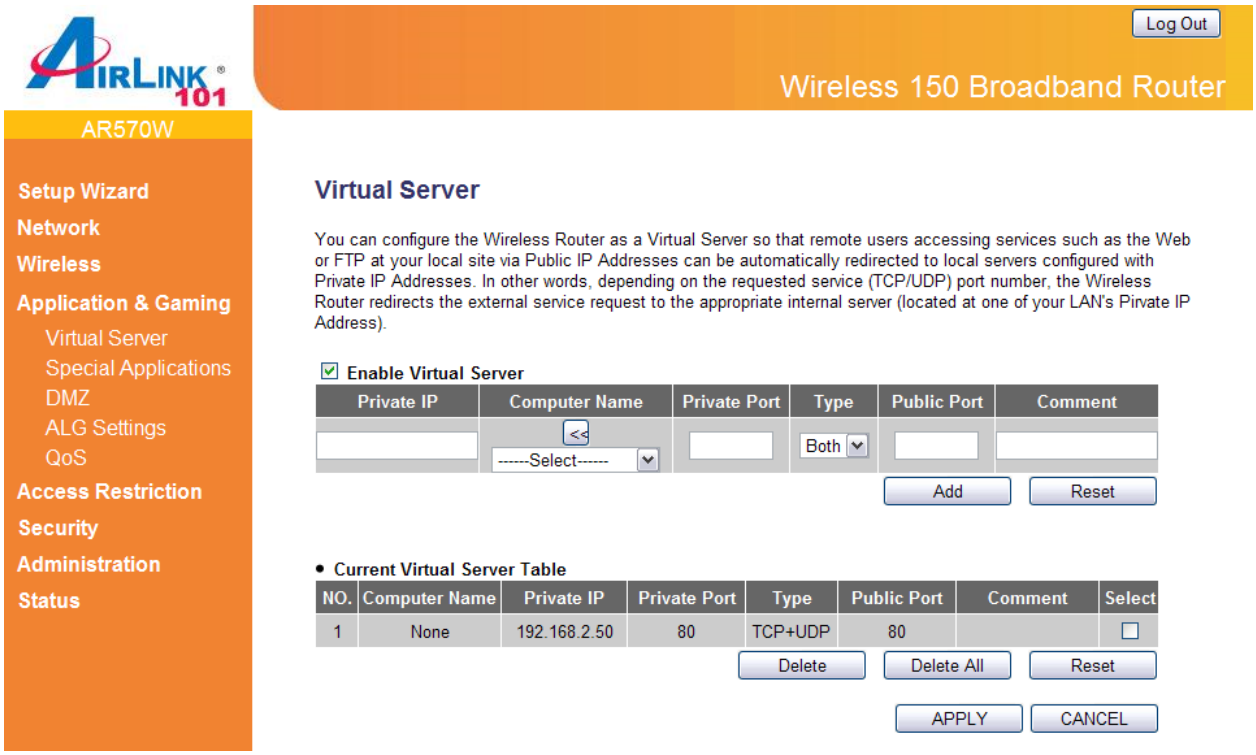
Parameters	Description
Enable WPS	Check this box to enable WPS function, uncheck it to disable WPS.
Wi-Fi Protected Setup Information	WPS-related system information will be displayed here: WPS Status: If the wireless security (encryption) function of this wireless router is properly set, you'll see "Configured" message here. If wireless security function has not been set, you'll see "unConfigured". Self PIN code: This is the WPS PIN code of this wireless router. This code is useful when you need to build wireless connection by WPS with other WPS-enabled wireless devices. SSID: The SSID of this wireless router will be displayed here. Authentication Mode: The wireless security authentication mode of this wireless router will be displayed here. If you don t enable security function of the wireless router before WPS is activated, the router will auto set the security to WPA (AES) and generate a set of passphrase key for WPS connection. Passphrase Key: The wireless security key of the router will be displayed here.
Config Mode	There are "Registrar" and "Enrollee" modes for the WPS connection. When "Registrar" is enabled, the wireless clients will follow the router's wireless settings for WPS connection. When "Enrollee" mode is enabled, the router will follow the wireless settings of wireless client for WPS connection.

Configure by Push Button	Click “Start PBC” to start Push-Button style WPS setup procedure. This wireless router will wait for WPS requests from wireless clients for 2 minutes. The “WLAN” LED on the wireless router will be steady on for 2 minutes when this wireless router is waiting for incoming WPS request.
Configure by Pin Code	Please input the PIN code of the wireless client you wish to connect, and click “Start PIN” button. The “WLAN” LED on the wireless router will be steady on when this wireless router is waiting for incoming WPS request.

3.3 Application & Gaming

3.3.1 Virtual Server (Port Forwarding)

The Virtual Server allows you to re-direct a particular range of service port numbers (from the Internet/WAN Ports) to a particular LAN IP address. It helps you to host some servers behind the router NAT firewall.

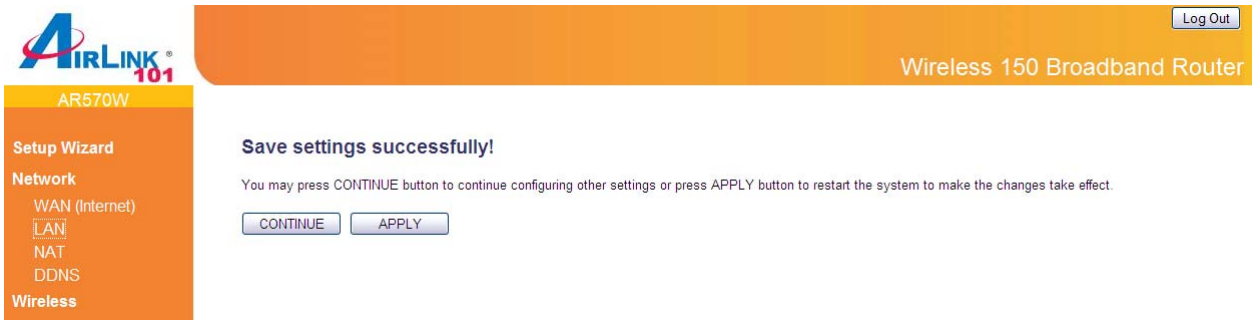


Parameter	Description
Enable Virtual Server	Enable Virtual Server (Port Forwarding)
Private IP	This is the private IP address of the server behind the NAT firewall. Note: You need to give your LAN PC clients a fixed/static IP address for Virtual Server to work properly.
Computer Name	Pull down the menu and all the computers connected to the router will be listed here. If you do not see any computer after you click on the drop-down menu, select the option "**Refresh**" and you will be given a list of computers that are connected to your network. You can easily select the computer name without checking the IP address of the computer.
Private Port	Input the port number of the IP address which provides Internet service.
Type	This is the protocol type to be forwarded. You can choose to forward "TCP" or "UDP" packets only or select "both" to forward both "TCP" and "UDP" packets.

Public Port	Input the port number of Internet IP address which will be redirected to the port number of local IP address defined above.
Comment	The description of this setting.
Current Virtual Server Table	From the table, you can check each Virtual Server setting.
Delete	If you want to delete a setting, check the 'select' box of the setting you want to delete, then click 'Delete' button. (You can select more than one setting).
Delete All	If you want to delete all settings listed here, please click 'Delete All' button.
Reset	You can also click 'Reset' button to unselect all.

After you finish with all settings, please click "Apply" button.
If you want to reset all settings in this page, please click "Cancel" button.

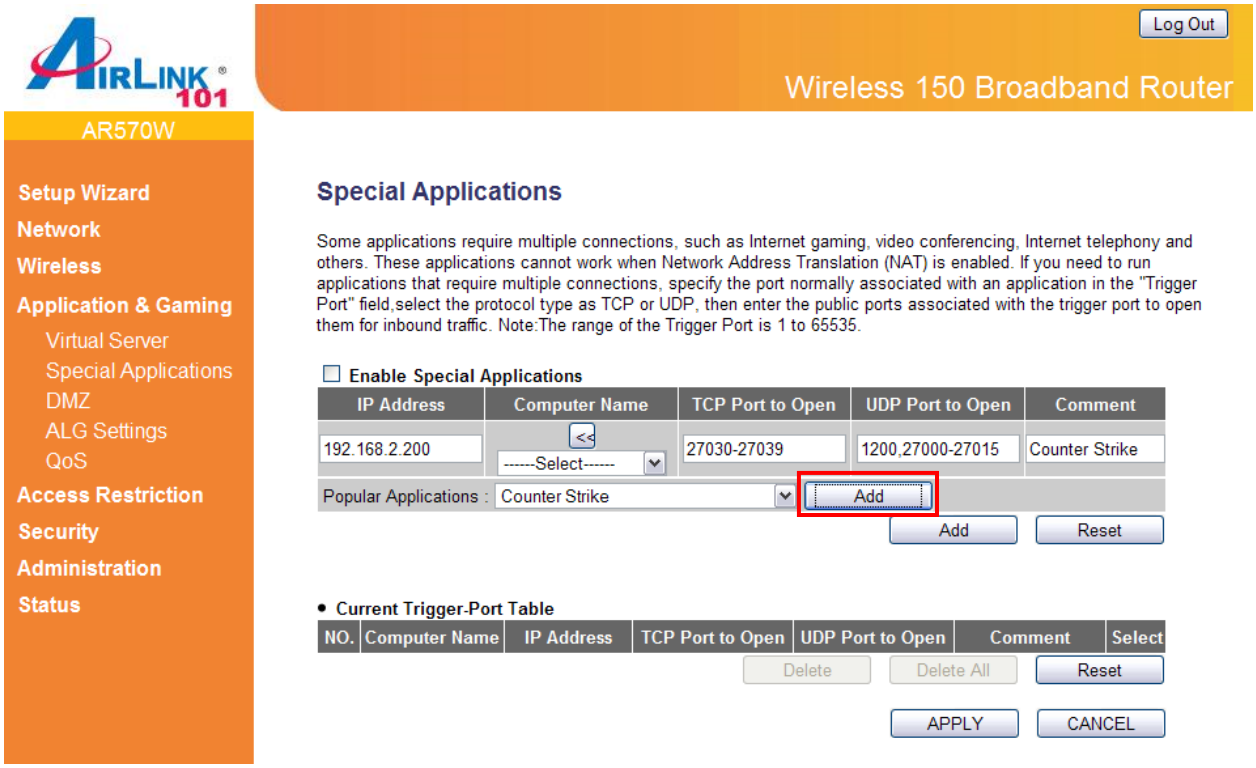
After you clicked Apply, the following message will be displayed on your web browser:



You can click "Continue" to back to previous setup page to continue on other setup procedures, or click "Apply" to reboot the router so the settings will take effect (Please wait for about 30 seconds while router is rebooting).

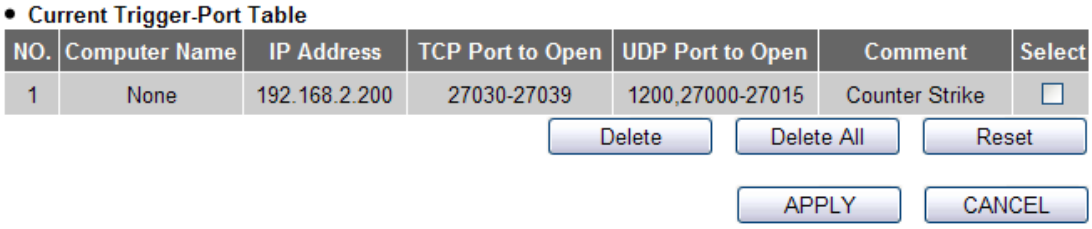
3.3.2 Special Applications (Port Triggering)

Some applications require multiple connections, such as Internet gaming, video conferencing, Internet telephony and others. These applications cannot work with simple Network Address Translation (NAT) rules. In this page, you can configure the Router to open certain TCP or UDP ports in order to make these applications work. Note: The range of the router ports is 1 to 65535.



Parameter	Description
Enable Special Applications	Check to enable Special Applications, or uncheck to disable.
IP Address	This is the private IP of the computer/server behind the NAT firewall. Note: You need to give your PC a fixed/static IP address for Special Applications to work properly.
Computer Name	This is the computer that you need to enable the Special Application function. Select a PC from here if you do not know its IP address and click on the << button to add the IP address to the left blank. If you do not see any computer after you click on the drop-down menu, select the option “Refresh” and you will be given a list of computers that are connected to your network.
TCP/UDP Port to Open	This is the TCP/UDP ports you want to trigger. Type in a range of TCP/UDP ports to be triggered. For instance, “5000-5300” or “9091, 9093-9100”, depending on your special application’s requirement.
Comment	The description of this setting.
Popular Application	This list includes many popular applications you may be using. Select the application you want to use and click on the Add button next to it; you will see the proper port numbers added to the “TCP/UDP Port to Open” blank.
Add (in red box)	Click on Add button in the red box to save the Special Application rule you set into the Current Trigger-Port Table.

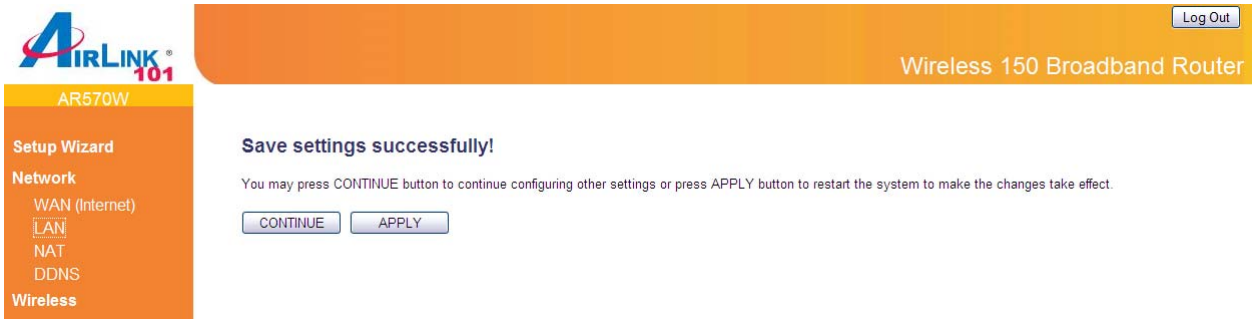
From the **Current Trigger-Port Table**, you can select each Special Application setting by checking the "Select" checkbox.



Parameter	Description
Delete	If you want to delete a setting, check the 'select' box of the setting you want to delete, then click 'Delete' button. (You can select more than one setting).
Delete All	If you want to delete all settings listed here, please click 'Delete All' button.
Reset	You can also click 'Reset' button to unselect all.

After you finish with all settings, please click "Apply" button.
If you want to reset all settings in this page, please click "Cancel" button.

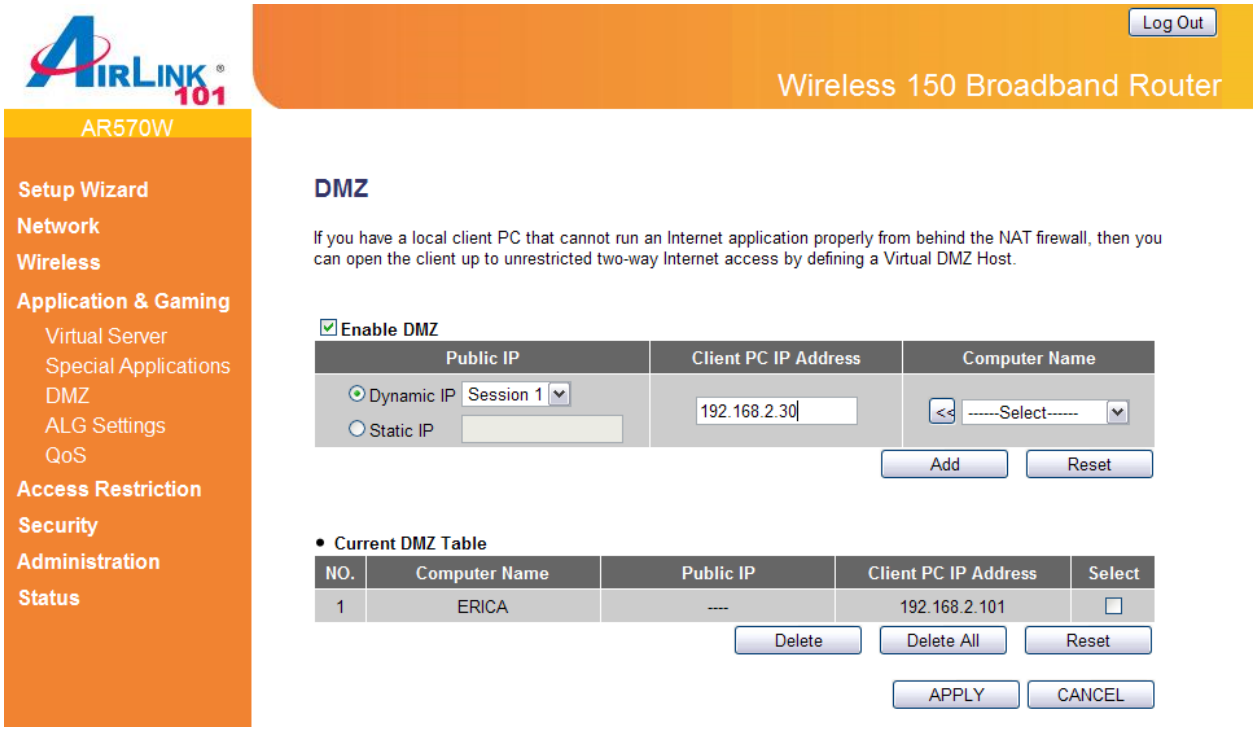
After you clicked Apply, the following message will be displayed on your web browser:



You can click "Continue" to back to previous setup page to continue on other setup procedures, or click "Apply" to reboot the router so the settings will take effect (Please wait for about 30 seconds while router is rebooting).

3.3.3 DMZ

If you have a local client PC that cannot run an Internet application (e.g. Games) properly from behind the NAT firewall, then you can open the client up to unrestricted two-way Internet access by defining a DMZ Host. The DMZ function allows you to re-direct all packets going to your WAN port IP address to a particular IP address in your LAN.

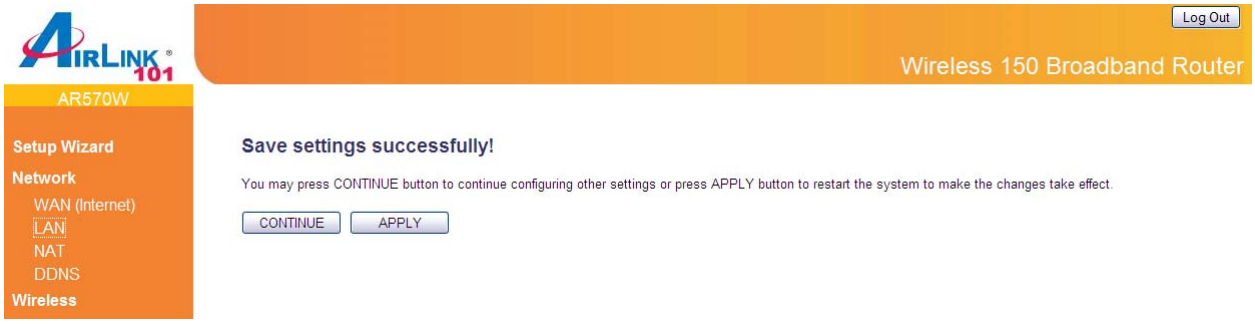


Parameter	Description
Enable DMZ	Check/uncheck to enable/disable DMZ.
Public IP	You can select “Dynamic IP” or “Static IP” here. If you select “Dynamic IP”, you have to select an Internet connection session from drop down menu; if you select “Static IP”, please input the IP address that you want to map to a specific private IP address.
Client PC IP address	Please input the private IP address that the Internet IP address will be mapped to.
Computer Name	Pull down the menu and all the computers connected to the router will be listed here. You can easily select the computer name without checking the IP address of the computer. If you do not see any computer after you click on the drop-down menu, select the option “Refresh” and you will be given a list of computers that are connected to your network.
Add	Click “Add” button to add the public IP address and associated private IP address to the DMZ table.
Reset	Click “Reset” to remove the value you inputted in Public IP address and Client PC IP address field.
Current DMZ Table	From the table, you can check each DMZ setting.
Delete	If you want to delete a setting, check the ‘select’ box of the setting you want to delete, then click ‘Delete’ button. (You can select more than one setting).
Delete All	If you want to delete all settings listed here, please click ‘Delete All’ button.

Reset	You can also click 'Reset' button to unselect all.

After you finish with all settings, please click "Apply" button.
If you want to reset all settings in this page, please click "Cancel" button.

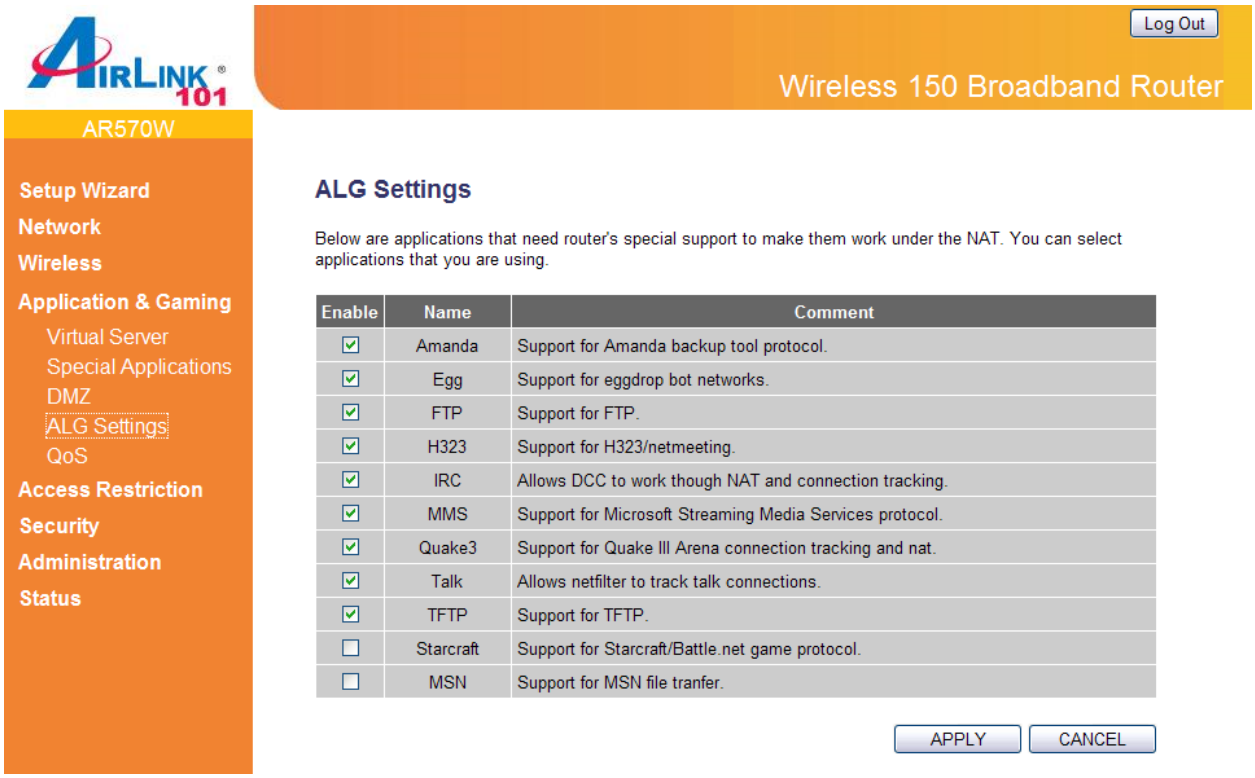
After you clicked Apply, the following message will be displayed on your web browser:



You can click "Continue" to back to previous setup page to continue on other setup procedures, or click "Apply" to reboot the router so the settings will take effect (Please wait for about 30 seconds while router is rebooting).

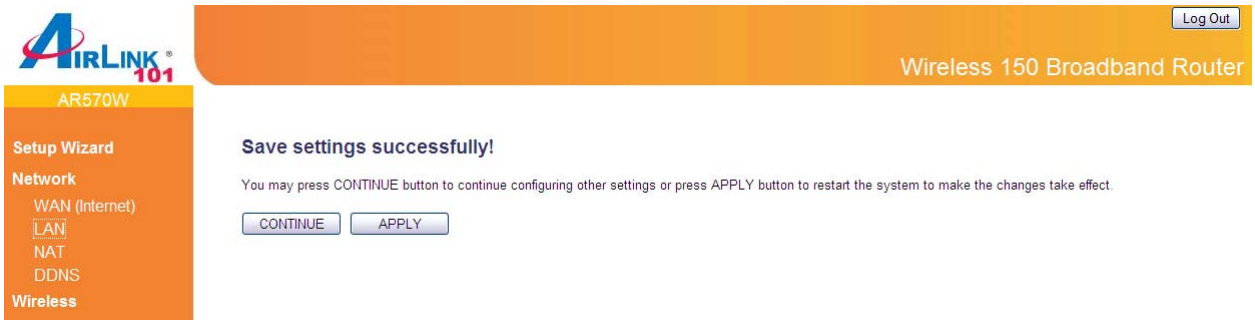
3.3.4 ALG Settings

Application Layer Gateway (ALG) is a special function of this router. It includes many preset routing rules for numerous applications which require special support. With these supports, those applications which required special support will be able to work with NAT architecture.



There are many applications listed here. Please check the box of the special support for applications you need.
After you finish with all settings, please click “Apply” button.
If you want to reset all settings in this page, please click “Cancel” button.

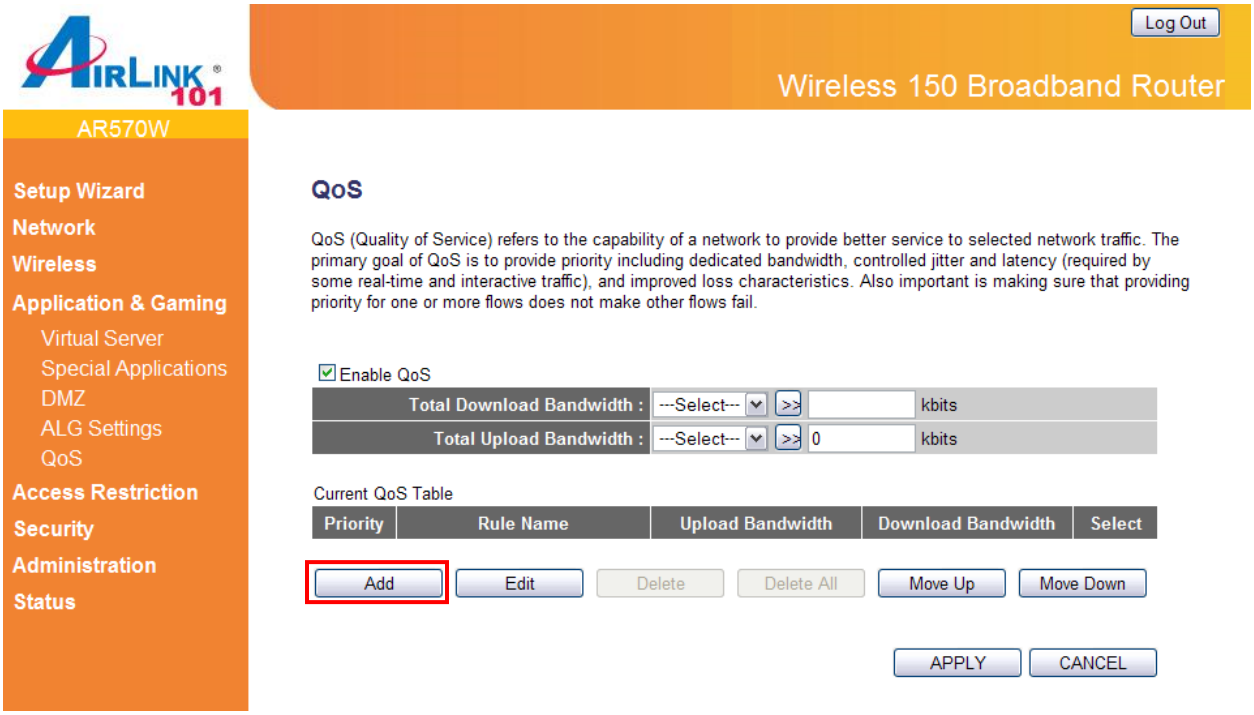
After you clicked Apply, the following message will be displayed on your web browser:



You can click “Continue” to back to previous setup page to continue on other setup procedures, or click “Apply” to reboot the router so the settings will take effect (Please wait for about 30 seconds while router is rebooting).

3.3.5 QoS

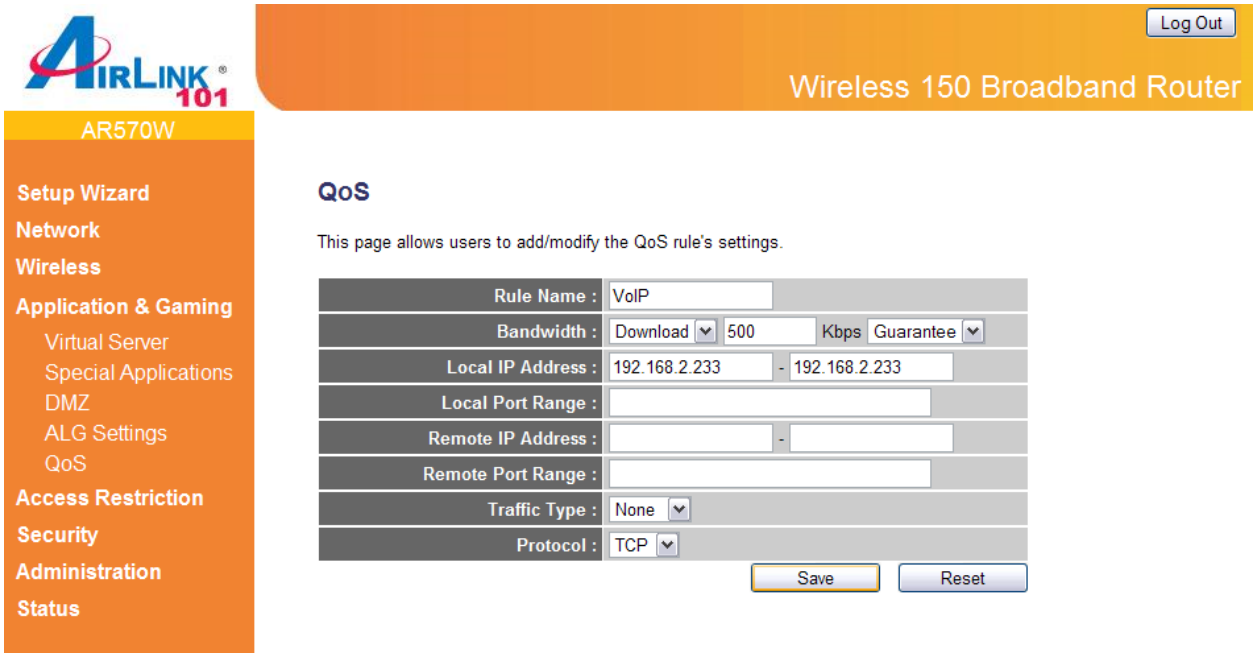
Quality of service, QoS provides an efficient way for computers on the network to share the internet bandwidth with a promised quality of internet service. Without QoS, all computers and devices on the network will compete with each other to get Internet bandwidth, and some applications which require guaranteed bandwidth (like video streaming and network telephone) will be affected, therefore an unpleasing result will occur, like the interruption of video / audio transfer.
With this function, you can limit the maximum bandwidth or give a guaranteed bandwidth for a specific computer, to avoid said unpleasing result from happening.



Parameter	Description
Enable QoS	Check this box to enable QoS, and uncheck this box to disable QoS.
Total Download Bandwidth	You can set the limit of total download bandwidth in kbits. To disable download bandwidth limitation, input **0** here.
Total Upload Bandwidth	You can set the limit of total upload bandwidth in kbits. To disable upload bandwidth limitation, input **0** here.
Current QoS Table	From the table, you can check each QoS rule setting.
Add	Click “Add” button to add a new QoS rule, see section 3.3.5.1 “Add a new QoS rule”“ below.
Edit	If you want to modify the content of a specific rule, please check its “Select”“ box, then click “Edit” button. Only one rule should be selected a time! If you didn’t select a rule before clicking “Edit” button, you’ll be prompted to add a new rule.
Delete	If you want to delete a setting, check the ‘select’ box of the setting you want to delete, then click ‘Delete’ button. (You can select more than one setting).
Delete All	If you want to delete all settings listed here, please click ‘Delete All’ button.
Move Up	You can raise the priority of the QoS rule you selected by clicking this button.
Move Down	You can lower the priority of the QoS rule you selected by clicking this button.

3.3.5.1 Add a new QoS rule

After you click “Add” button on QoS page, the following message will appear:



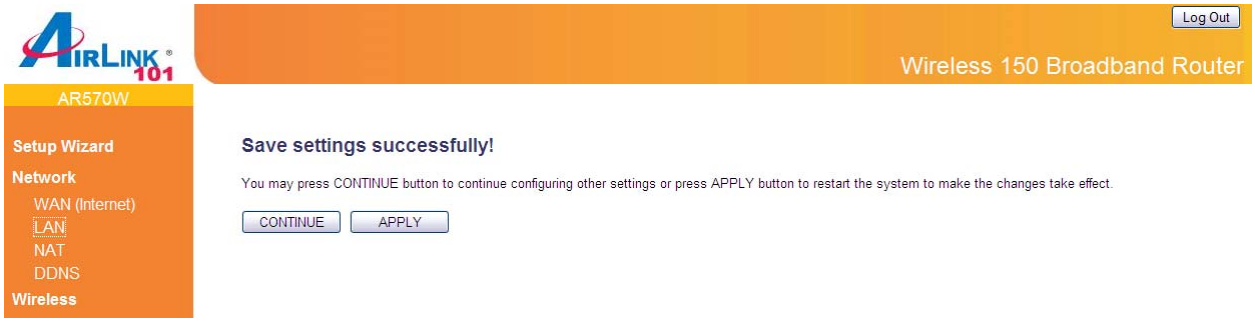
Parameter	Description
Rule Name	Please give a name to this QoS rule (up to 15 alphanumerical characters).
Bandwidth	Set the bandwidth limitation of this QoS rule. You have to select the data direction of this rule (Upload of Download), and the speed of bandwidth limitation in Kbps, then select the type of QoS: “guarantee”" (guaranteed usable bandwidth for this rule) or “max” (set the maximum bandwidth for the application allowed by this rule).
Local IP Address	Specify the local (source) IP address that will be affected by this rule. Please input the starting IP address in the left field, and input the end IP address in the right field to define a range of IP addresses, or just input the IP address in the left field to define a single IP address.
Local Port Range	Please input the range of local (source) port numbers that will be affected by this rule. If you want to apply this rule on port 80 to 90, please input "80-90"; if you want to apply this rule on a single port, just input the port number, such as 80.
Remote IP Address	Specify the remote (destination) IP address that will be affected by this rule. Please input the starting IP address in the left field, and input the end IP address in the right field to define a range of IP addresses, or just input the IP address in the left field to define a single IP address.
Remote Port Range	Please input the range of remote (destination) port number that will be affected by this rule. If you want to apply this rule on port 80 to 90, please input "80-90"; if you want to apply this rule on a single port, just input the port number, such as 80". If the remote (destination) IP address and /or port number is universal, just leave it blank.

Traffic Type	Please select the traffic type of this rule, available options are None, SMTP, HTTP, POP3, and FTP. You can select a specific traffic type for this rule, if you want to make this rule as a IP address based rule (apply the limitation on all traffics from / to the specified IP address / port number), select “None”.
Protocol	Please select the protocol type of this rule, available options are TCP and UDP. If you don"t know what protocol your application uses, please try “TCP” first, and switch to “UDP” if this rule doesn’t seems to work.

After you finish with all settings, please click “Save” button, you’ll be brought back to previous menu, and the rule you just set will appear in current QoS table; if you did anything wrong, you’ll get an error message when you click “Save” button, please correct your input by the instructions given by the error message.

After you finish with all QoS settings, please click “Apply” button.
If you want to reset all settings in this page, please click “Cancel” button.

After you clicked Apply, the following message will be displayed on your web browser:



You can click “Continue” to back to previous setup page to continue on other setup procedures, or click “Apply” to reboot the router so the settings will take effect (Please wait for about 30 seconds while router is rebooting).

3.4 Access Restrictions

This function allows you to configure some Internet access rules for your local computers based on the IP address, applications, URL or keywords.

3.4.1 IP & Port Filtering

If you want to restrict users from accessing certain Internet applications/services (e.g. Internet websites, email, FTP etc.) by their IP addresses, then you can set up the filtering rules here. Entries in this table are restricted to use certain type of connections from the router. IP filters can be helpful in securing or restricting your local network.

Log Out
Wireless 150 Broadband Router
AR570W
Setup Wizard
Network
Wireless
Application & Gaming
Access Restriction
IP & Port Filtering
MAC Filtering
URL Filtering
Security
Administration
Status
IP & Port Filtering
IP & Port Filtering allows users to define the traffic type permitted or not permitted in your LAN. You can control which PC client uses what services in which they can have access to these services. If both of IP & Port filtering and MAC filtering are enabled simultaneously, the MAC filtering table will be checked first and then IP & Port filtering table.
Enable IP & Port Filtering
Deny
Allow
NO.
Client PC Description
Client PC IP Address
Client Service
Protocol
Port Range
Select
Add PC
Delete
Delete All
APPLY
CANCEL

Parameters	Description
Enable IP & Port Filtering	Check/uncheck to enable/disable the IP & Port Filtering.
Deny/Allow	Please select “Deny” or “Allow” to decide the behavior of IP filtering table. If you select deny, all IP addresses listed in filtering table will be denied from connecting to the network; if you select allow, only IP addresses listed in filtering table will be able to connect to the network, and all other network devices will be rejected.
Add PC	Click “Add PC” to add a new IP address to IP filtering table. See more information below.
Delete	If you want to delete a specific setting, check the ‘select’ box of the setting you want to delete, then click ‘Delete’ button. (You can select more than one setting).
Delete All	If you want to delete all settings listed here, please click ‘Delete All’ button.

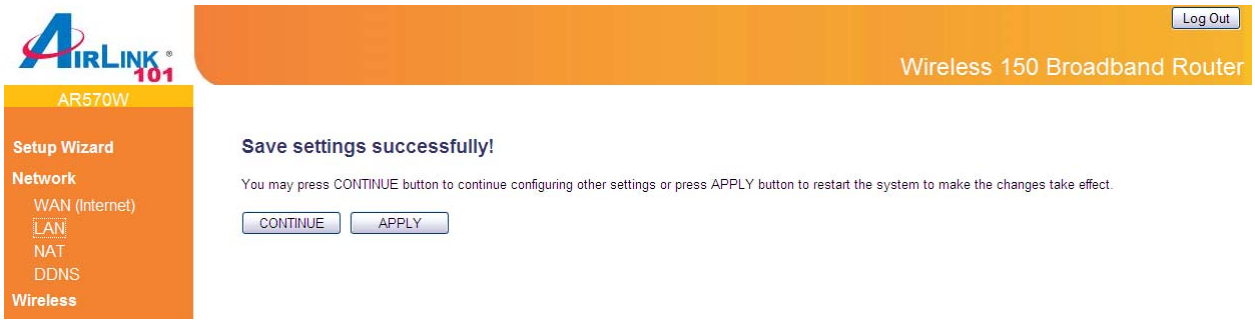
Click **Add PC** to add a new IP address to IP filtering table, up to 20 IP addresses can be added.

Parameters	Description
Client PC Description	Please input any text to describe this IP address, up to 16 alphanumerical characters.
Client PC IP address	Please input the starting IP address in the left field, and input the end IP address in the right field to define a range of IP addresses, or just input the IP address in the left field to define a single IP address.
Client Service	Please check all services you want to allow or deny this IP address to use, you can check multiple services.
Protocol	If the service you need is not listed above, you can create a new service on your own. Please select TCP or UDP, if you're not sure, please select "Both".

Port Range	Please input the port range of new service here. If you want to specify port 80 to 90, please input “80-90”; if you want to apply this rule on a single port, just input the port number, such as 80.
Add	When you finish with all settings, please click “Add” to save settings, you’ll be brought back to previous menu, and the rule you just set will appear in current IP filtering table.

After you finish with all settings, please click “Apply” button.
If you want to reset all settings in this page, please click “Cancel” button.

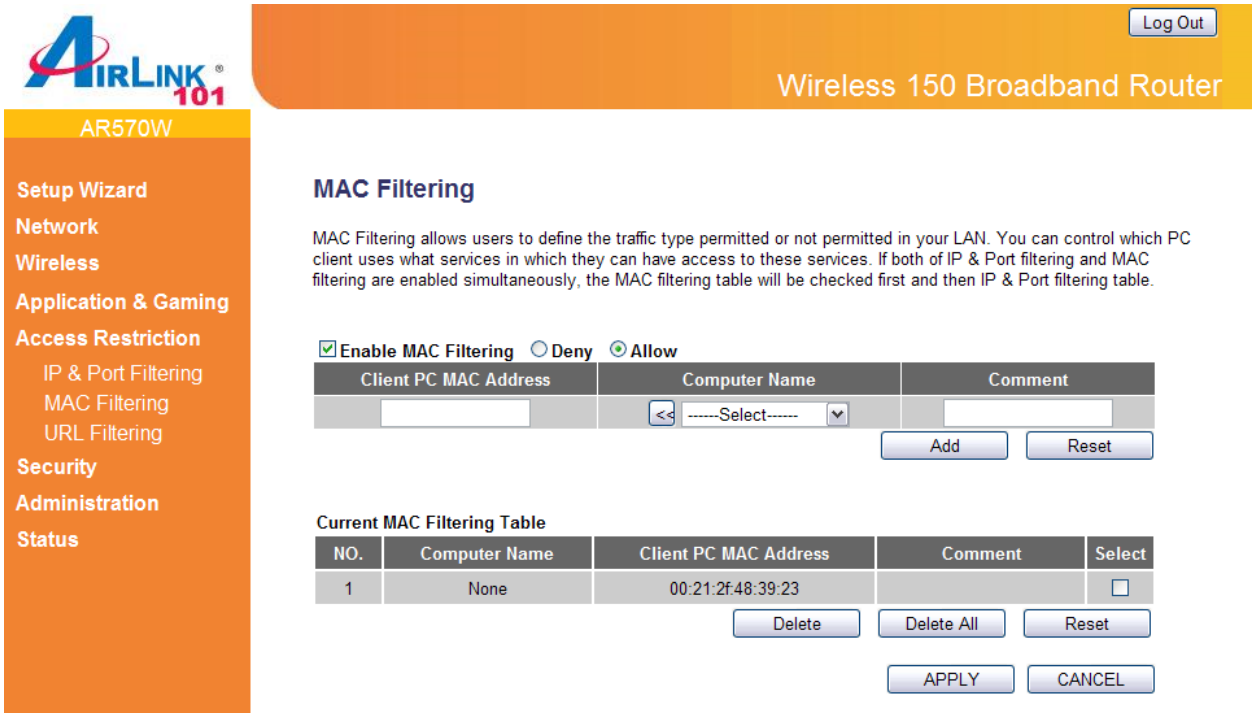
After you clicked Apply, the following message will be displayed on your web browser:



You can click “Continue” to back to previous setup page to continue on other setup procedures, or click “Apply” to reboot the router so the settings will take effect (Please wait for about 30 seconds while router is rebooting).

3.4.2 MAC Filtering

If you want to restrict users from accessing certain Internet applications/services (e.g. Internet websites, email, FTP etc.) by their MAC addresses, then you can set up the filtering rules here.

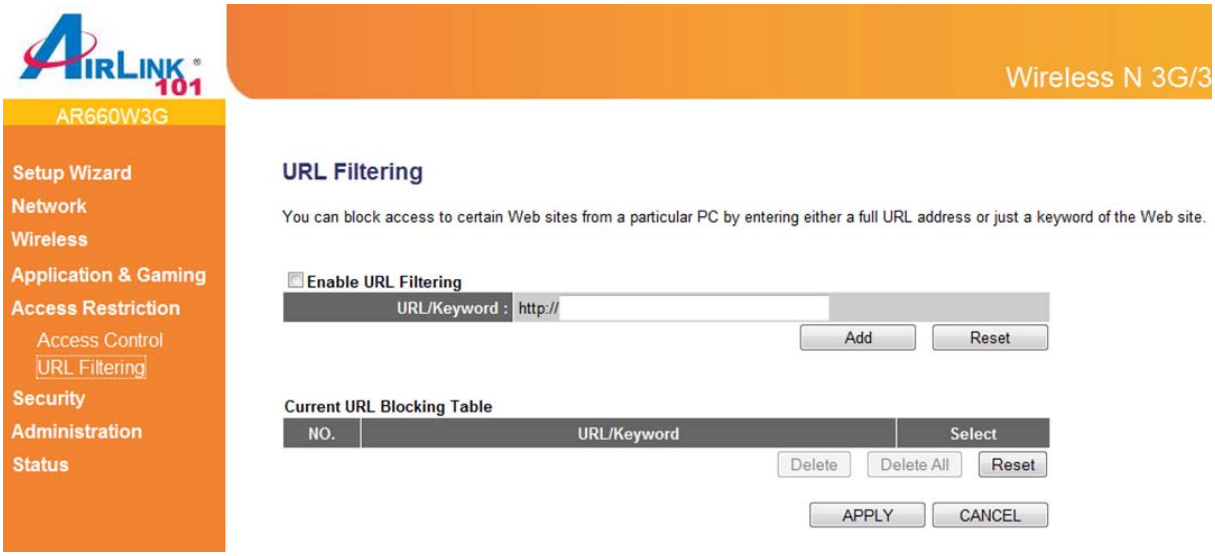


Parameters	Description
Enable MAC Filtering	Check this box to enable the MAC filtering function. Please select “Deny” or “Allow” to decide the behavior of MAC filtering table. If you select Deny, all MAC addresses listed in filtering table will be denied from connecting to the network; if you select Allow, only MAC addresses listed in filtering table will be able to connect to the network, and all other network devices are rejected.
Client PC MAC Address	Input the MAC address of the devices you want to filter in format ‘xx:xx:xx:xx:xx:xx’.
Computer Name	Pull down the menu and all the computers connected to the router will be listed here. You can easily select the computer name without checking the IP address of the computer. If you do not see any computer after you click on the drop-down menu, select the option “Refresh” and you will be given a list of computers that are connected to your network
Comment	You can input any text here as the comment of this MAC address, like ‘ROOM 2A Computer’.
Add	Click “Add” button to add the MAC address and associated comment to the MAC address filtering table.
Reset	Remove all inputted values.
Current MAC Filtering Table	From the table, you can check each MAC Address filter setting.
Delete	If you want to delete a specific MAC address entry, check the ‘select’ box of the MAC address you want to delete, then click ‘Delete’ button. (You can select more than one MAC addresses).

Delete All	If you want to delete all MAC addresses listed here, please click 'Delete All' button.
Reset	You can also click 'Reset' button to unselect all.

3.4.3 URL/Keyword Filtering

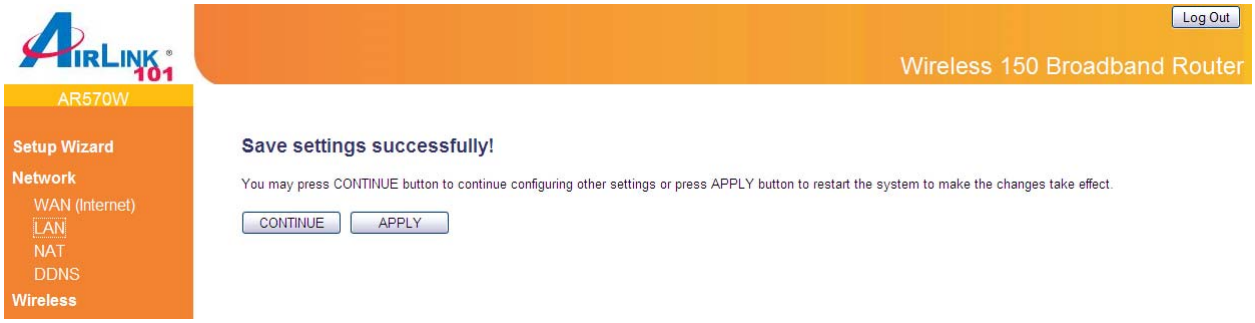
You can block access to certain websites or web contents from local PCs by entering a full URL address or just keywords about the web contents. This filter can help parents to manage the Internet usage for their children (i.e. Parental Control).



Parameter	Description
Enable URL Filtering	Enable/Disable URL Blocking.
URL/Keyword	You can enter the full URL address of a website or any **keyword** of certain web contents you want to block.
Current URL Blocking Table	From the table, you can check each URL filter setting.
Delete	If you want to delete a setting, check the 'select' box of the setting you want to delete, then click 'Delete' button. (You can select more than one setting).
Delete All	If you want to delete all settings listed here, please click 'Delete All' button.
Reset	You can also click 'Reset' button to unselect all.

After you finish with all settings, please click "Apply" button.
If you want to reset all settings in this page, please click "Cancel" button.

After you clicked Apply, the following message will be displayed on your web browser:

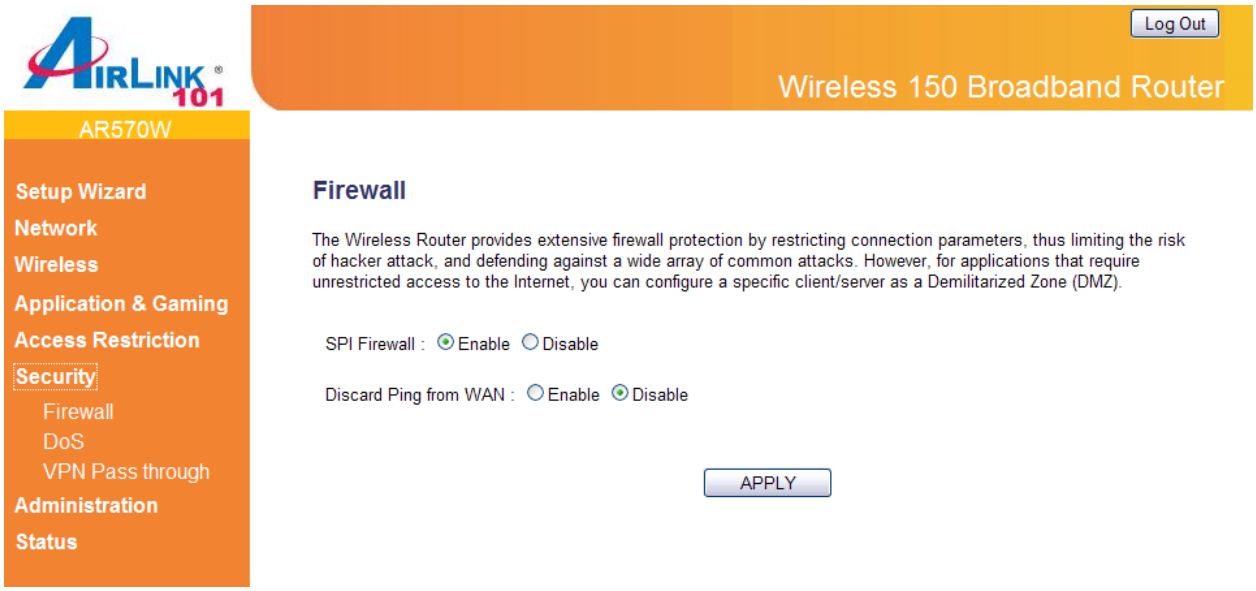


You can click “Continue” to back to previous setup page to continue on other setup procedures, or click “Apply” to reboot the router so the settings will take effect (Please wait for about 30 seconds while router is rebooting).

3.5 Security

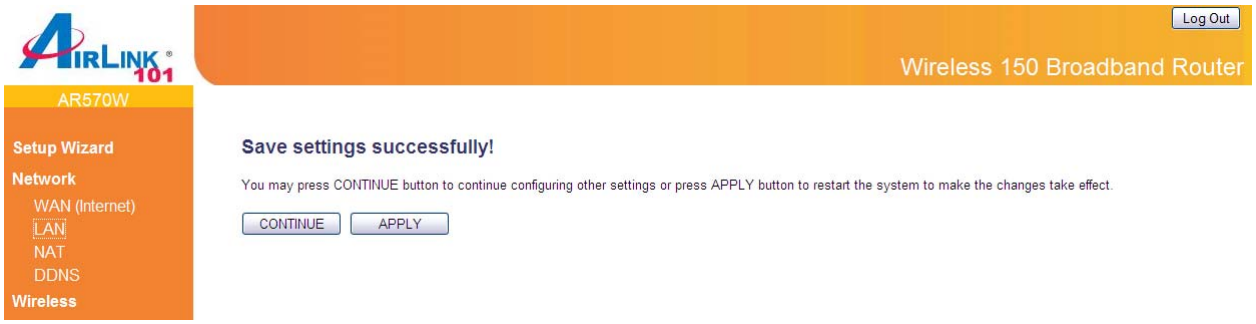
3.5.1 Firewall

Excepting NAT, this router also provides firewall function to block malicious intruders from accessing your computers on local network. These functions include inbound attack prevention, and block outbound traffics.
The Wireless 150 Router AR570W has built in **SPI Firewall** which is a type of firewall that inspects incoming data packets to make sure they correspond to an outgoing request. Unsolicited and possibly harmful packets are rejected. It is suggested to keep SPI Firewall enabled.
When you enable “Discard Ping from WAN”, you router will not respond to a “ping” request or to its WAN interface.


Log Out
Wireless 150 Broadband Router
AR570W
Setup Wizard
Network
Wireless
Application & Gaming
Access Restriction
Security
Firewall
DoS
VPN Pass through
Administration
Status
Firewall
The Wireless Router provides extensive firewall protection by restricting connection parameters, thus limiting the risk of hacker attack, and defending against a wide array of common attacks. However, for applications that require unrestricted access to the Internet, you can configure a specific client/server as a Demilitarized Zone (DMZ).
SPI Firewall : Enable Disable
Discard Ping from WAN : Enable Disable
APPLY

Please select “Enable” or “Disable to enable or disable SPI Firewall and Discard Ping from WAN function of this router. Click “Apply” to save the settings you made.
After you finish with all settings, please click “Apply” button.
If you want to reset all settings in this page, please click “Cancel” button.

After you clicked Apply, the following message will be displayed on your web browser:

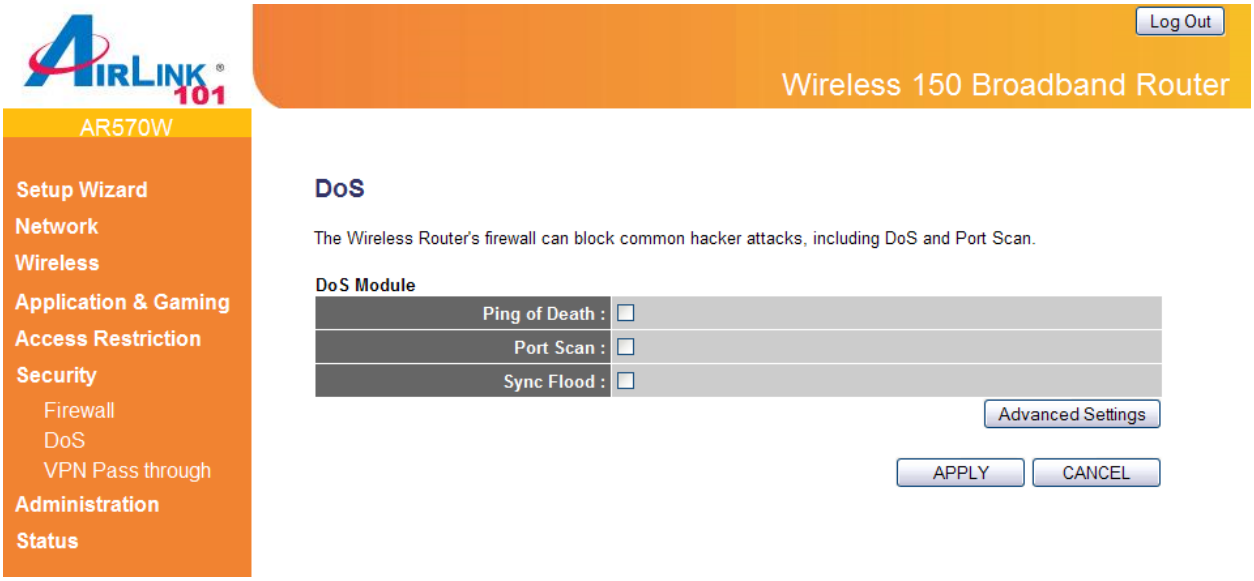


You can click “Continue” to back to previous setup page to continue on other setup procedures, or click “Apply” to reboot the router so the settings will take effect (Please wait for about 30 seconds while router is rebooting).

3.5.2 DoS (Denial-of-Service)

Denial of Service (DoS) is a common attack measure, by transmitting a great amount of data or request to your Internet IP address and server, the Internet connection will become very slow, and server may stop responding because it is not capable to handle too much traffics.

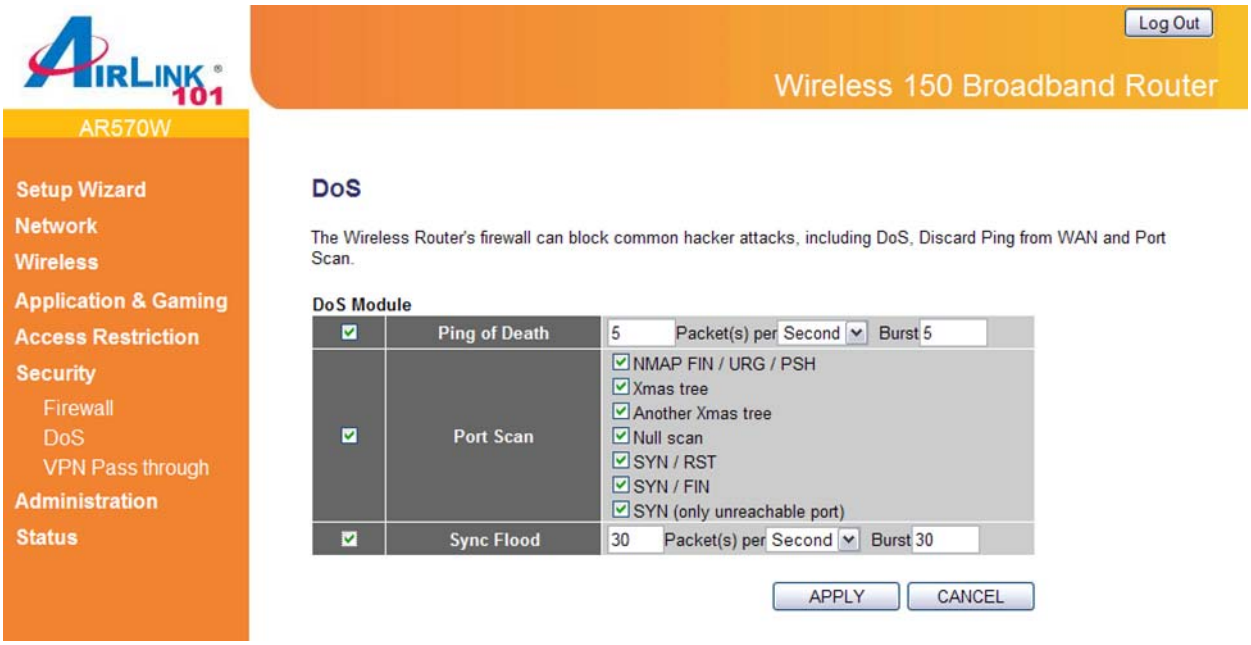
This router has a built-in DoS attack prevention mechanism; when you activate it, the router will stop the DoS attack for you.



Parameter	Description
Ping of Death	Set the threshold of when this DoS prevention mechanism will be activated. Please check the box of Ping of Death, and input the frequency of threshold (how many packets per second, minute, or hour), you can also input the "Burst" value, which means when this number of "Ping of Death" packet is received in very short time, this DoS prevention mechanism will be activated.
Discard Ping From WAN	Check the box to discard this ping request to the WAN IP address of the router.
Port Scan	Many kind of port scan methods are listed here, please check one or more DoS attack methods you want to prevent.
Sync Flood	Like Ping of Death, you can set the threshold of when this DoS prevention mechanism will be activated.
Advanced Settings	Click this button and you can set advanced settings of the DoS prevention method listed above, please see section 3.5.2.1 'DoS – Advanced Settings' below.

3.5.2.1 DoS – Advanced Settings

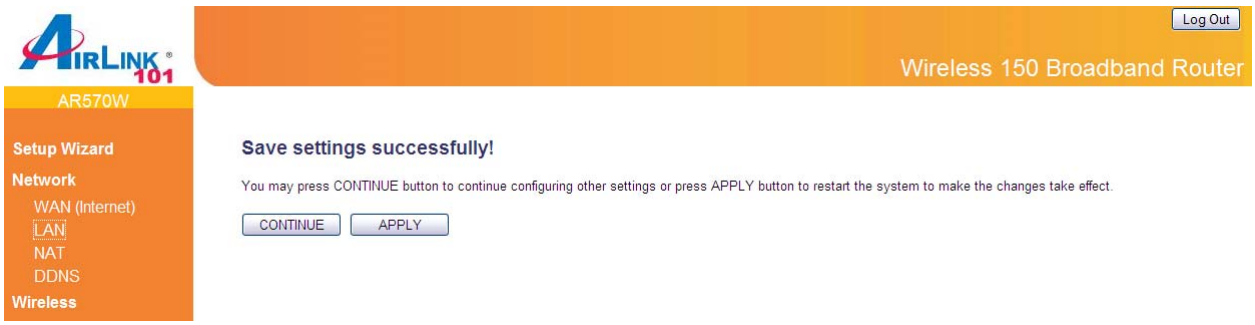
When you click 'Advanced Settings' button in DoS page, the following page will be displayed on your web browser:



Parameter	Description
Ping of Death	Set the threshold of when this DoS prevention mechanism will be activated. Please check the box of Ping of Death, and input the frequency of threshold (how many packets per second, minute, or hour), you can also input the 'Burst' value, which means when this number of 'Ping of Death' packet is received in very short time, this DoS prevention mechanism will be activated.
Port Scan	Many kind of port scan methods are listed here, please check one or more DoS attack methods you want to prevent.
Sync Flood	Like Ping of Death, you can set the threshold of when this DoS prevention mechanism will be activated.

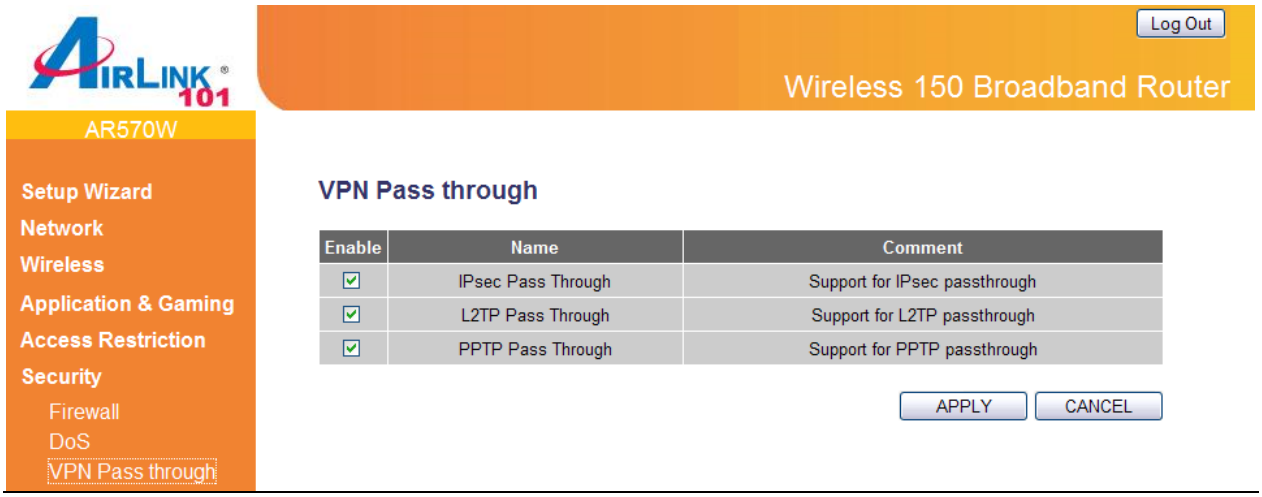
After you finish with all settings, please click "Apply" button.
If you want to reset all settings in this page, please click "Cancel" button.

After you clicked Apply, the following message will be displayed on your web browser:



You can click “Continue” to back to previous setup page to continue on other setup procedures, or click “Apply” to reboot the router so the settings will take effect (Please wait for about 30 seconds while router is rebooting).

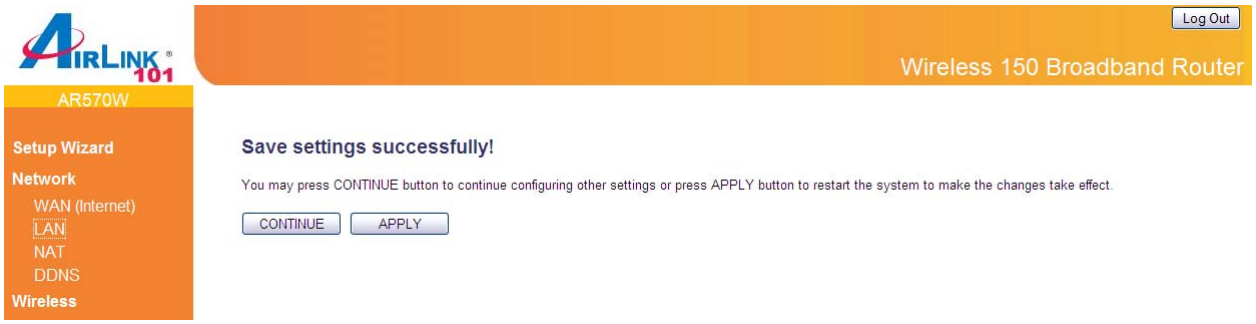
3.5.3 VPN Pass through



Parameter	Description
IPsec pass through	Check this box and the router will enable IPsec packets pass through the router for VPN connection.
PPTP pass through	Check this box and the router will enable PPTP packets pass through the router for VPN connection
L2TP pass through	Check this box and the router will enable L2TP packets pass through the router for VPN connection.

After you finish with all settings, please click “Apply” button.
If you want to reset all settings in this page, please click “Cancel” button.

After you clicked Apply, the following message will be displayed on your web browser:

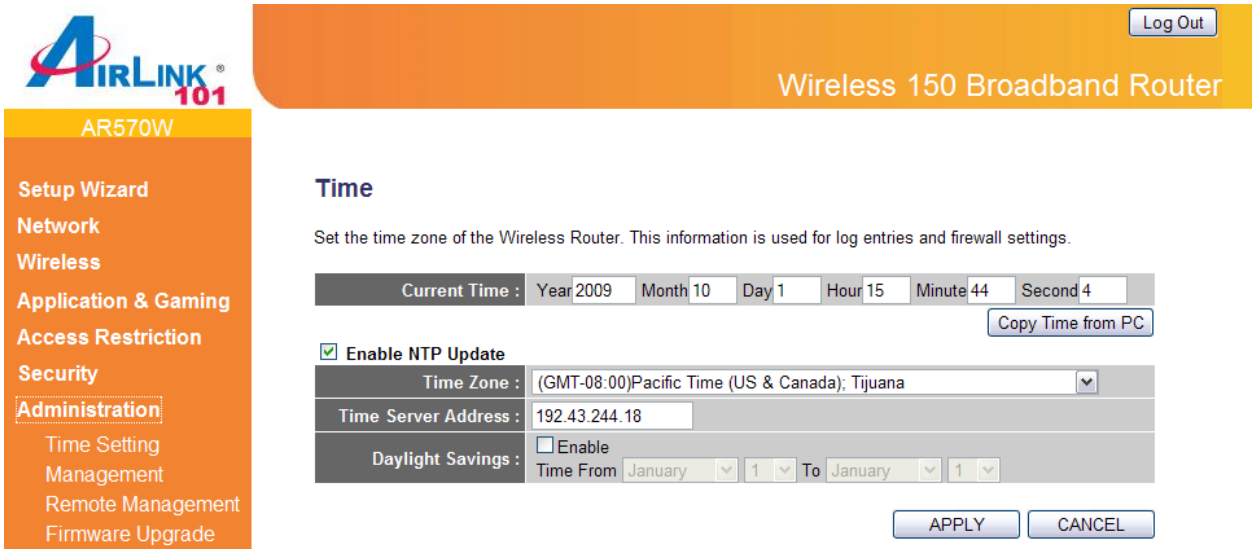


You can click “Continue” to back to previous setup page to continue on other setup procedures, or click “Apply” to reboot the router so the settings will take effect (Please wait for about 30 seconds while router is rebooting).

3.6 Administration

The Administration page allows you to specify a time zone, to change the system password and to specify a remote management port, to upgrade firmware, to save/reload configuration settings, to enable system log, to view the statistics information, and to enable/disable UPnP for the Router.

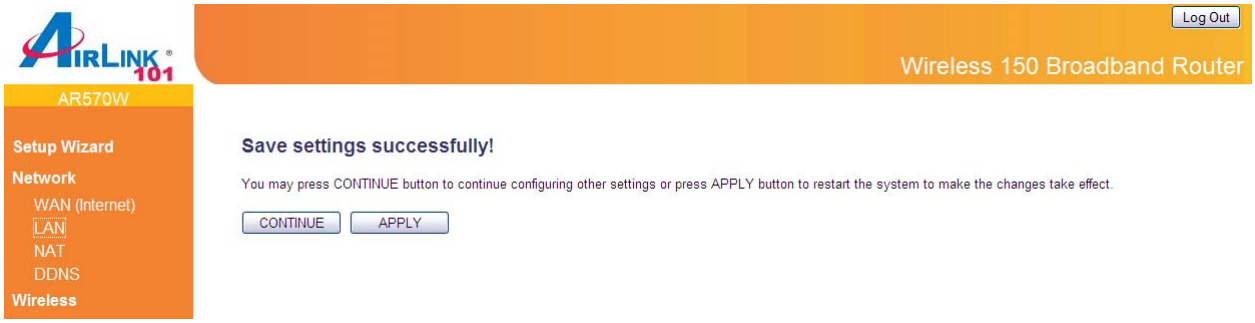
3.6.1 Time



Parameter	Description
Current Time	Display the router's current time. You can manually configure it or Click on Copy Time from PC.
Enable NTP Update	Check to enable time auto-synchronization through Internet.
Time Zone	You can select your local time zone here. The router will sync time according to your time zone selection.
Time Server Address	Input the IP address / host name of time server here
Daylight Savings	If the country you live uses daylight saving, please check the Enable box and choose the duration of daylight saving.

After you finish with all settings, please click "Apply" button.
If you want to reset all settings in this page, please click "Cancel" button.

After you clicked Apply, the following message will be displayed on your web browser:

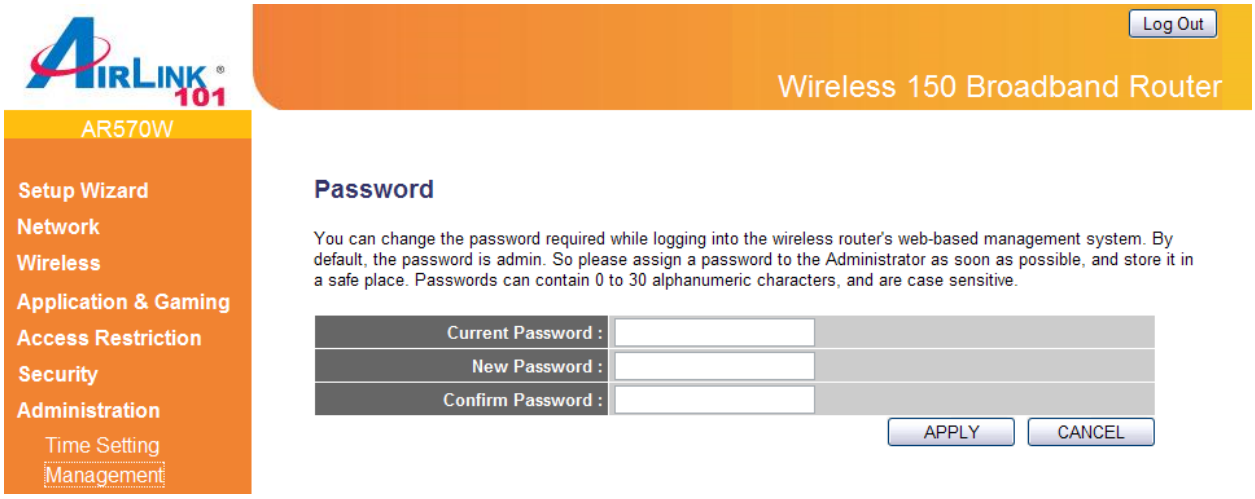


You can click “Continue” to back to previous setup page to continue on other setup procedures, or click “Apply” to reboot the router so the settings will take effect (Please wait for about 30 seconds while router is rebooting).

3.6.2 Management

3.6.2.1 Password

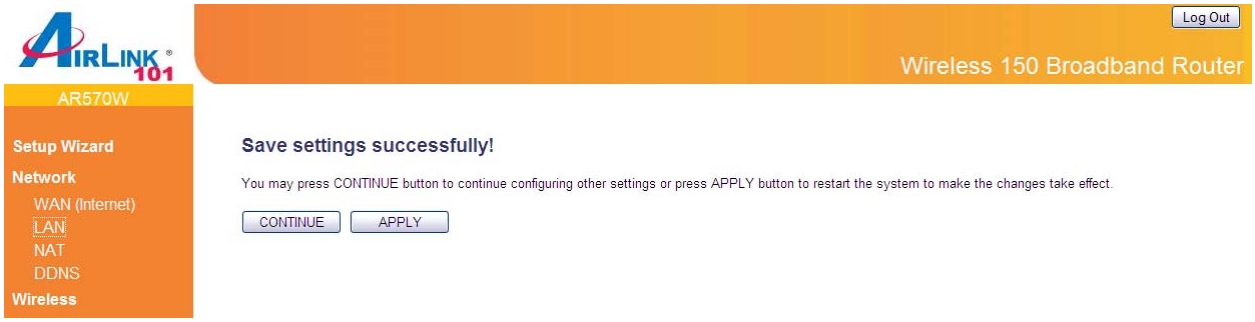
You can change the password required to log into the Router’s web configuration utility. The default user name and password are “admin”. It is suggested to change the administrator’s default password as soon as you start to use the Router, and store it in a safe place. The password can consist of 0 to 12 alphanumeric characters, and are case sensitive.


Log Out
Wireless 150 Broadband Router
AR570W
Setup Wizard
Network
Wireless
Application & Gaming
Access Restriction
Security
Administration
Time Setting
Management
Password
You can change the password required while logging into the wireless router's web-based management system. By default, the password is admin. So please assign a password to the Administrator as soon as possible, and store it in a safe place. Passwords can contain 0 to 30 alphanumeric characters, and are case sensitive.
Current Password :
New Password :
Confirm Password :
APPLY
CANCEL

Parameters	Description
Current Password	Enter the current password of the router.
New Password	Enter your new password.
Confirmed Password	Enter your new password again for verification purposes. **Note**: If you forget your password, you’ll have to reset the router to the factory default (user name and password are both ‘admin’) by pushing and holding the reset button on the back of the router for 10 seconds.

After you finish with all settings, please click “Apply” button.
If you want to reset all settings in this page, please click “Cancel” button.

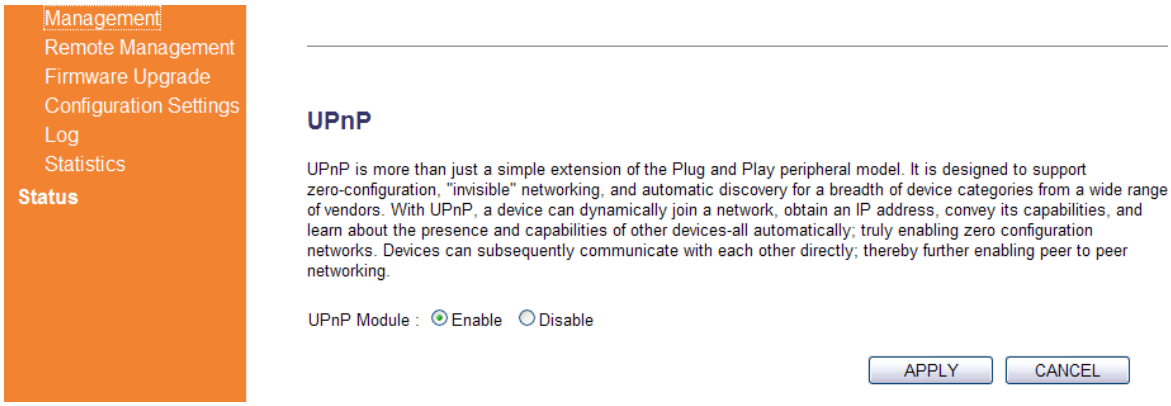
After you clicked Apply, the following message will be displayed on your web browser:



You can click “Continue” to back to previous setup page to continue on other setup procedures, or click “Apply” to reboot the router so the settings will take effect (Please wait for about 30 seconds while router is rebooting).

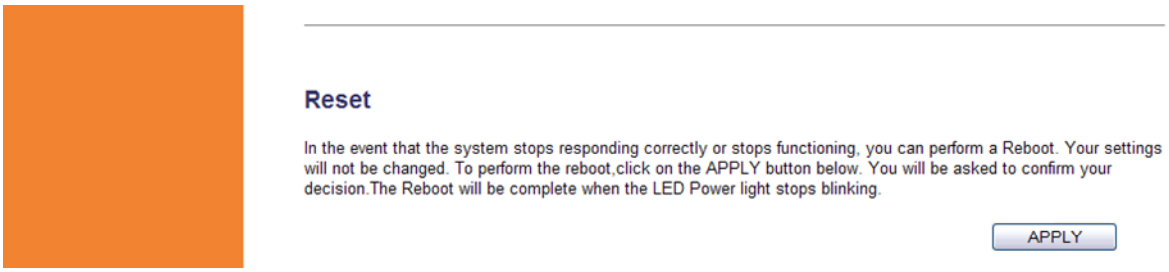
3.6.2.2 UPnP

You can select enable or disable UPnP feature here. After you enable the UPnP feature, all client systems that support UPnP, like Windows Vista, can discover this router automatically.


Management
Remote Management
Firmware Upgrade
Configuration Settings
Log
Statistics
Status
UPnP
UPnP is more than just a simple extension of the Plug and Play peripheral model. It is designed to support zero-configuration, "invisible" networking, and automatic discovery for a breadth of device categories from a wide range of vendors. With UPnP, a device can dynamically join a network, obtain an IP address, convey its capabilities, and learn about the presence and capabilities of other devices-all automatically; truly enabling zero configuration networks. Devices can subsequently communicate with each other directly; thereby further enabling peer to peer networking.
UPnP Module : Enable Disable
APPLY
CANCEL

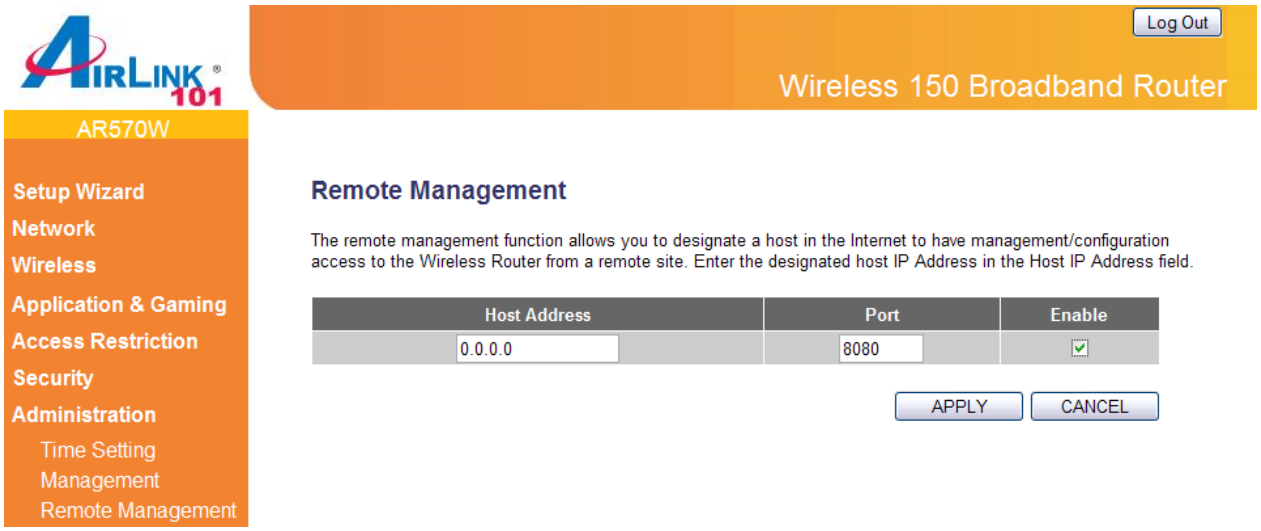
3.6.2.3 Reset (Reboot)

Click Apply button under the Reset section if you want to reboot the router.


Reset
In the event that the system stops responding correctly or stops functioning, you can perform a Reboot. Your settings will not be changed. To perform the reboot,click on the APPLY button below. You will be asked to confirm your decision.The Reboot will be complete when the LED Power light stops blinking.
APPLY

3.6.3 Remote Management

You can manage this router remotely by enabling the ‘Remote Management’ function.

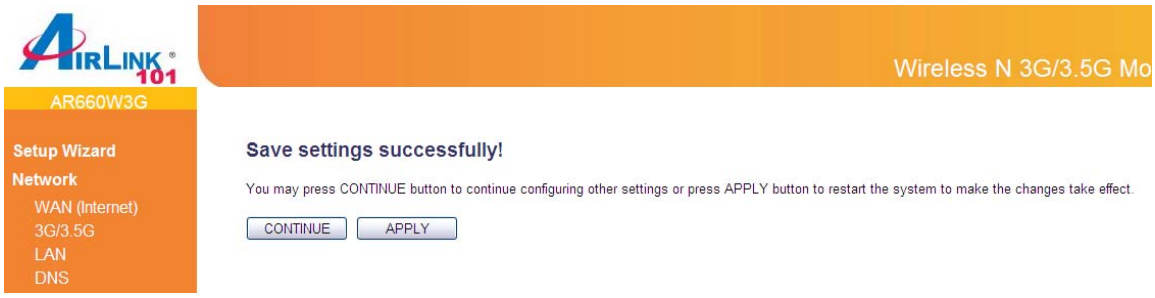


Parameters	Description
Host Address	Input the IP address of the remote host you wish to initiate a management access. “0.0.0.0” means any remote IP address. If you specify an IP address here, then the router will only allow remote access from this specific IP address.
Port	You can define the port number this router should expect an incoming request. If you’re providing a web service (default port number is 80), you should try to use other port number. You can use the default port setting “8080”, or something like “32245” or “1429”. (Any integer between 1 and 65534)
Enabled	Select the field to start the configuration

After you finish with all settings, please click “Apply” button.
If you want to reset all settings in this page, please click “Cancel” button.

To access your router remotely, you need to enter the router’s WAN IP address in a web browser with specific port number. For example, your router’s WAN IP address is 67.39.100.32 (you can find the WAN IP address at **Status > Internet Connection > IP Address**), and the port number is 8080. You need to go to http://67.39.100.32:8080 to access your router.

After you clicked Apply, the following message will be displayed on your web browser:

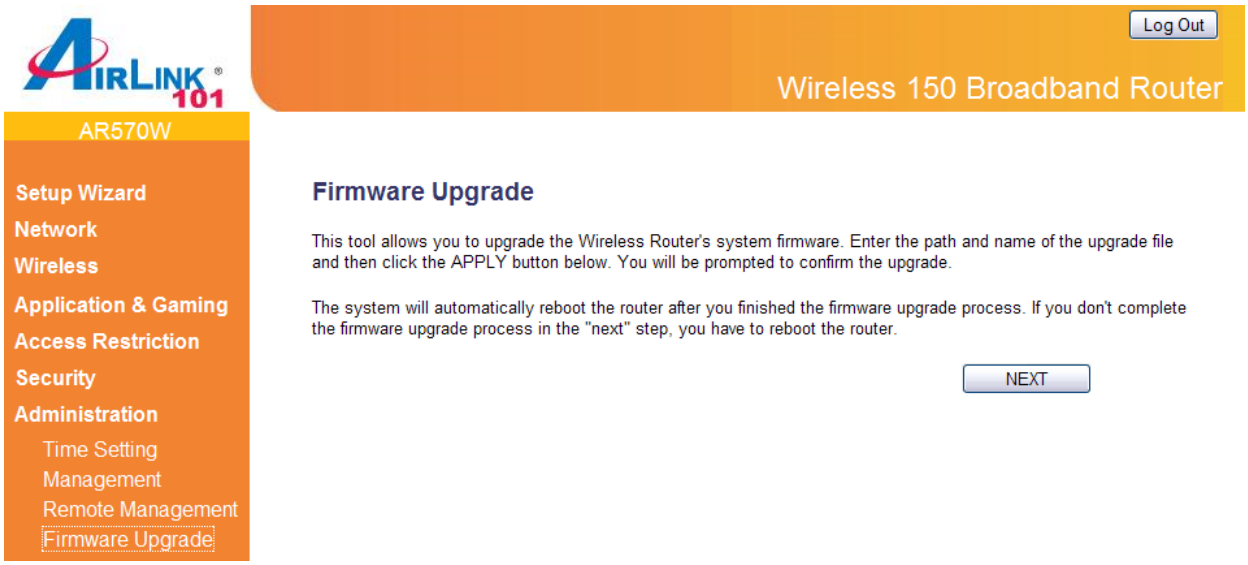


You can click “Continue” to back to previous setup page to continue on other setup procedures, or click “Apply” to reboot the router so the settings will take effect (Please wait for about 30 seconds while router is rebooting).

3.6.4 Firmware Upgrade

To upgrade the firmware for the Router, you need to download the firmware file and save it to your local hard disk first. You may need to unzip it if it is a .zip file.

Click **NEXT** to start the firmware upgrade.

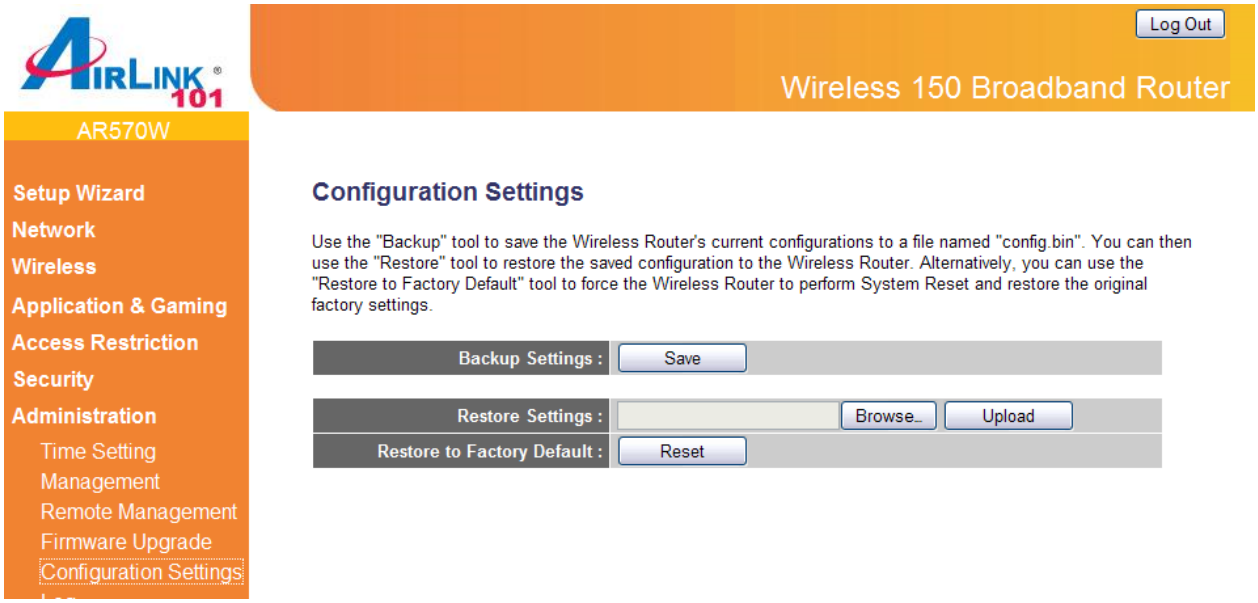

Log Out
Wireless 150 Broadband Router
AR570W
Setup Wizard
Network
Wireless
Application & Gaming
Access Restriction
Security
Administration
Time Setting
Management
Remote Management
Firmware Upgrade
Firmware Upgrade
This tool allows you to upgrade the Wireless Router's system firmware. Enter the path and name of the upgrade file and then click the APPLY button below. You will be prompted to confirm the upgrade.
The system will automatically reboot the router after you finished the firmware upgrade process. If you don't complete the firmware upgrade process in the "next" step, you have to reboot the router.
NEXT

Click on **Browse** to select the firmware you just downloaded/unzipped, then click **APPLY** to start the upgrade process. (You may have to wait a few minutes for the upgrade to complete).

NOTE: Never interrupt the upgrade process by closing the web browser or physically disconnect your computer from router. If the firmware you uploaded is corrupt, the firmware upgrade will fail, and you may contact Airlink101 Technical Support for help.

3.6.5 Configuration Settings

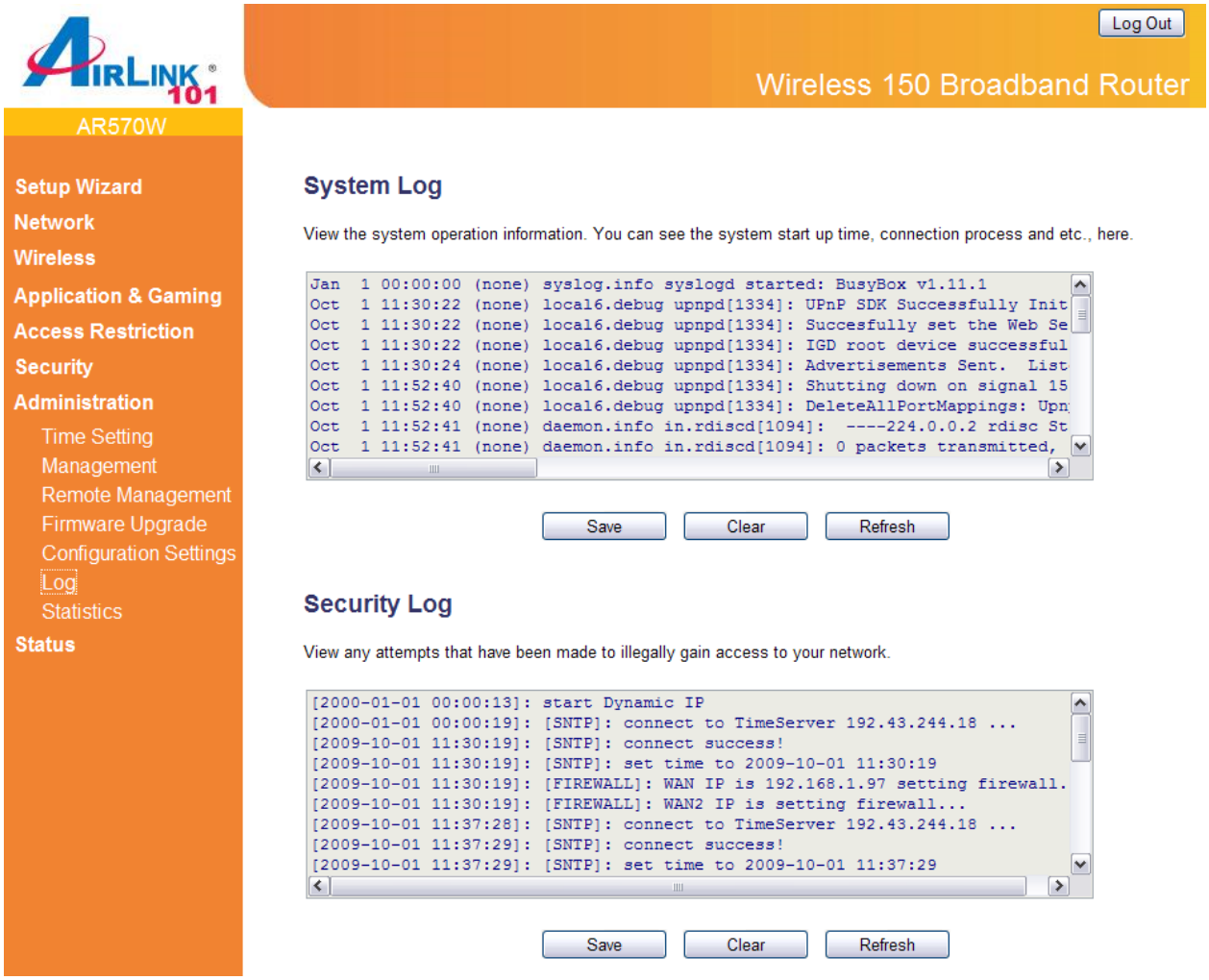
The Configuration Settings screen allows you to save (**Backup**) the router's current configuration setting. Saving the configuration settings provides an added protection and convenience should problems occur with the router and you have to reset to factory default. When you save the configuration settings (Backup) you can re-load the saved settings into the router through the **Restore** function. If extreme problems occur you can use the **Restore to Factory Default** function, this will set all configurations to its original default settings (e.g. when you first purchased the router).


Log Out
Wireless 150 Broadband Router
AR570W
Setup Wizard
Network
Wireless
Application & Gaming
Access Restriction
Security
Administration
Time Setting
Management
Remote Management
Firmware Upgrade
Configuration Settings
Configuration Settings
Use the "Backup" tool to save the Wireless Router's current configurations to a file named "config.bin". You can then use the "Restore" tool to restore the saved configuration to the Wireless Router. Alternatively, you can use the "Restore to Factory Default" tool to force the Wireless Router to perform System Reset and restore the original factory settings.
Backup Settings :
Save
Restore Settings :
Browse...
Upload
Restore to Factory Default :
Reset

Parameters	Description
Backup Settings	Click Save button to save the router's current configuration to a file named "config.bin" on your PC.
Restore Settings	Click "Browse" button to locate the file you have saved before and click "Upload" button to restore the saved configuration to the Broadband router.
Restore to Factory Default	Click Reset button if you want to force the router restore the original factory settings.

3.6.6 Log

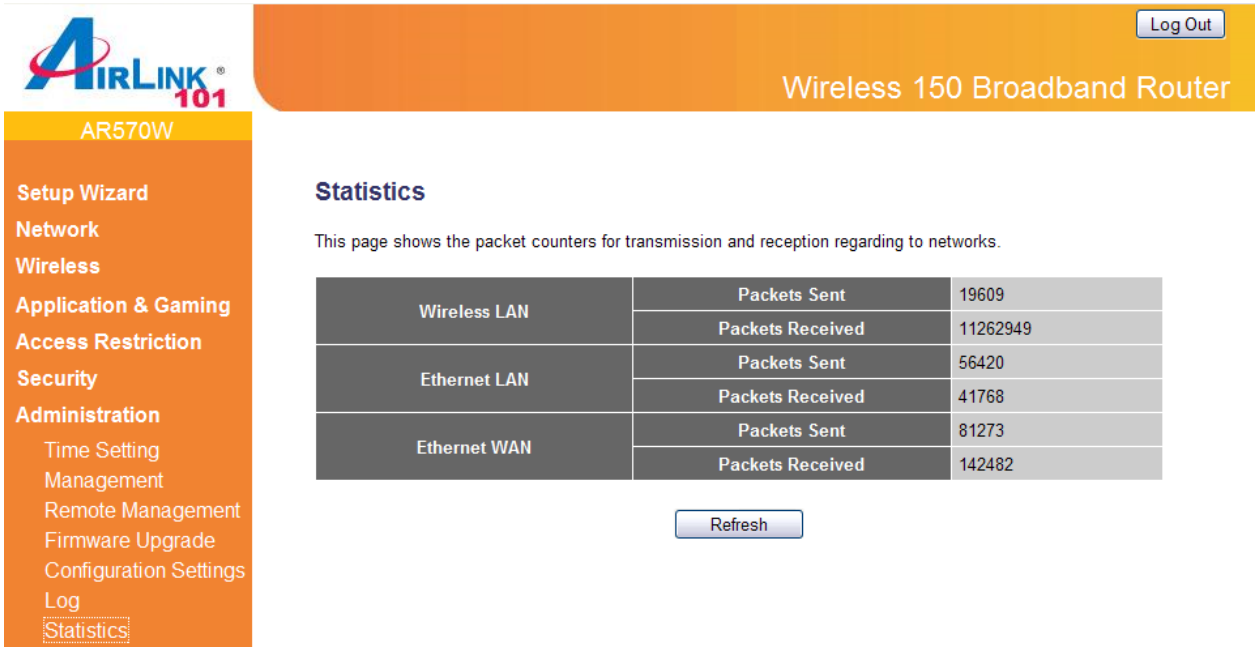
All important system events and system security are logged. You can use this function to check the log of your router.


Log Out
Wireless 150 Broadband Router
AR570W
Setup Wizard
Network
Wireless
Application & Gaming
Access Restriction
Security
Administration
Time Setting
Management
Remote Management
Firmware Upgrade
Configuration Settings
Log
Statistics
Status
System Log
View the system operation information. You can see the system start up time, connection process and etc., here.
Jan 1 00:00:00 (none) syslog.info syslogd started: BusyBox v1.11.1
Oct 1 11:30:22 (none) local6.debug upnpd[1334]: UPnP SDK Successfully Init
Oct 1 11:30:22 (none) local6.debug upnpd[1334]: Succesfully set the Web Se
Oct 1 11:30:22 (none) local6.debug upnpd[1334]: IGD root device successful
Oct 1 11:30:24 (none) local6.debug upnpd[1334]: Advertisements Sent. List
Oct 1 11:52:40 (none) local6.debug upnpd[1334]: Shutting down on signal 15
Oct 1 11:52:40 (none) local6.debug upnpd[1334]: DeleteAllPortMappings: Upn
Oct 1 11:52:41 (none) daemon.info in.rdiscd[1094]: ----224.0.0.2 rdisc St
Oct 1 11:52:41 (none) daemon.info in.rdiscd[1094]: 0 packets transmitted,
Save
Clear
Refresh
Security Log
View any attempts that have been made to illegally gain access to your network.
[2000-01-01 00:00:13]: start Dynamic IP
[2000-01-01 00:00:19]: [SNTP]: connect to TimeServer 192.43.244.18 ...
[2009-10-01 11:30:19]: [SNTP]: connect success!
[2009-10-01 11:30:19]: [SNTP]: set time to 2009-10-01 11:30:19
[2009-10-01 11:30:19]: [FIREWALL]: WAN IP is 192.168.1.97 setting firewall.
[2009-10-01 11:30:19]: [FIREWALL]: WAN2 IP is setting firewall...
[2009-10-01 11:37:28]: [SNTP]: connect to TimeServer 192.43.244.18 ...
[2009-10-01 11:37:29]: [SNTP]: connect success!
[2009-10-01 11:37:29]: [SNTP]: set time to 2009-10-01 11:37:29
Save
Clear
Refresh

Parameters	Description
Save	Save current event log to a text file.
Clear	Delete all event logs displayed here.
Refresh	Refresh the event log display.

3.6.7 Statistics

View the statistics of packets sent and received on WAN, LAN and Wireless LAN.



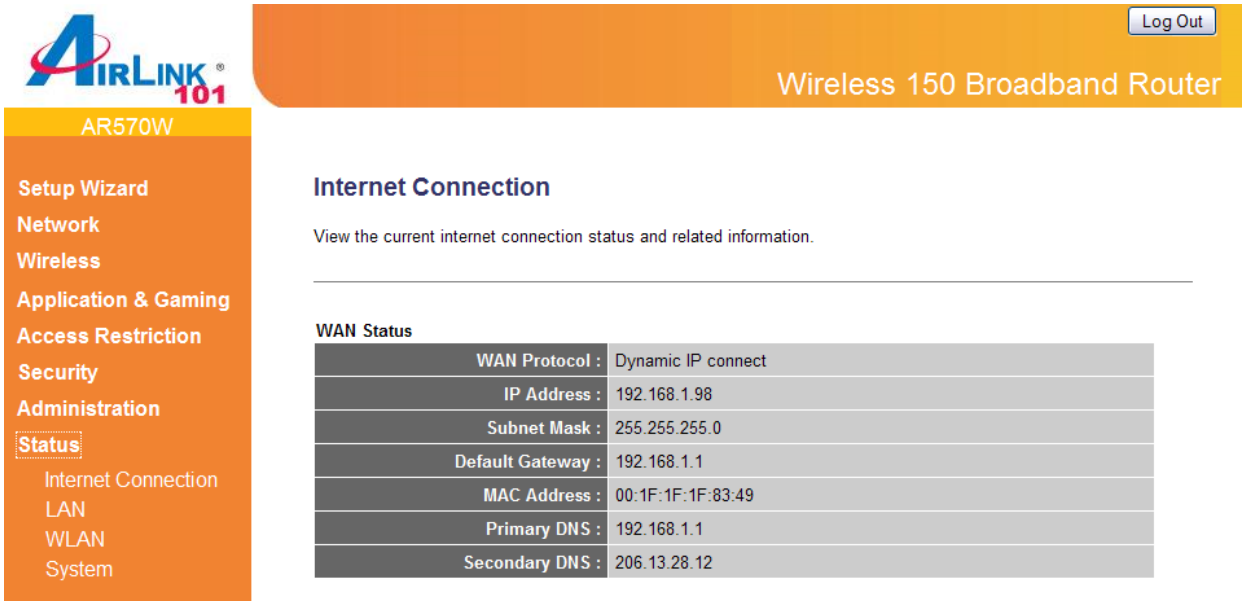
Click Refresh to display the latest information.

3.7 Status

The Status section allows you to monitor the current status of your router. You can use the Status page to monitor: the Internet, LAN connection, Wireless status, and the current firmware version of the Router.

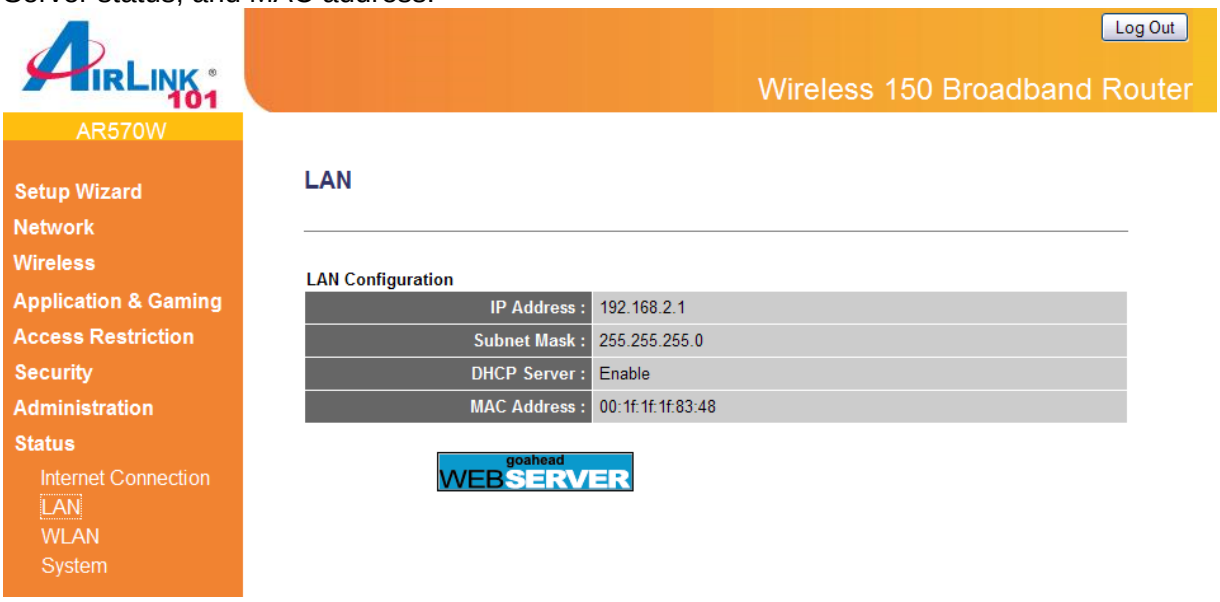
3.7.1 Internet Connection Status

You can use this function to view the status of current Internet connection.



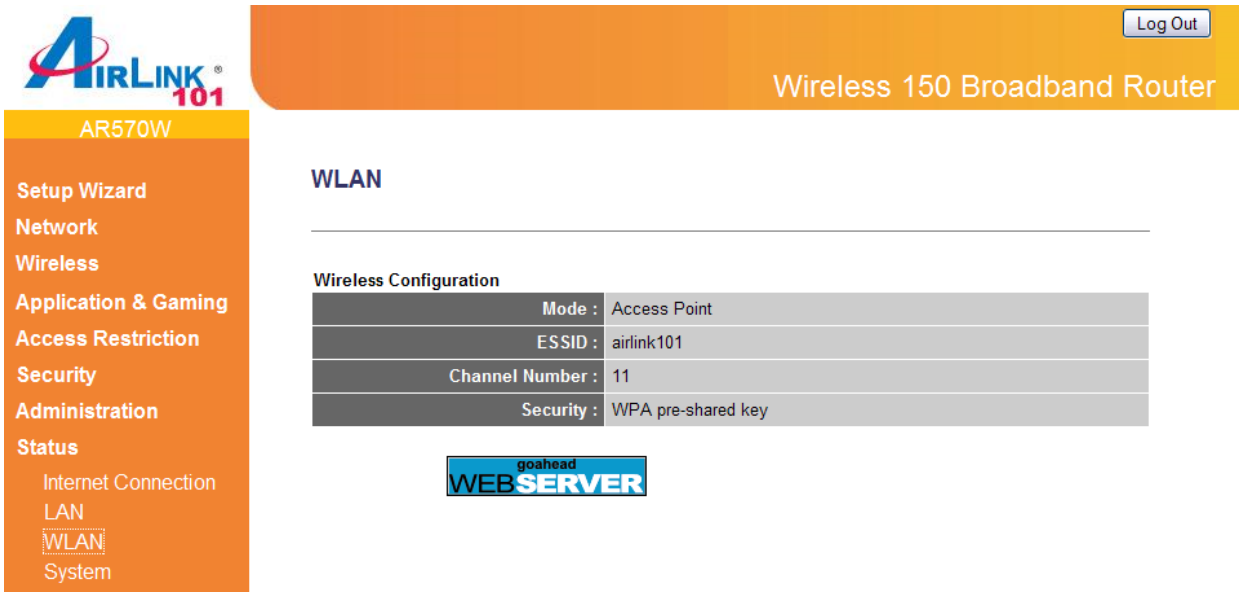
3.7.2 LAN Status

You can use this function to view the LAN status of your router, including TCP/IP setting, DHCP Server status, and MAC address.



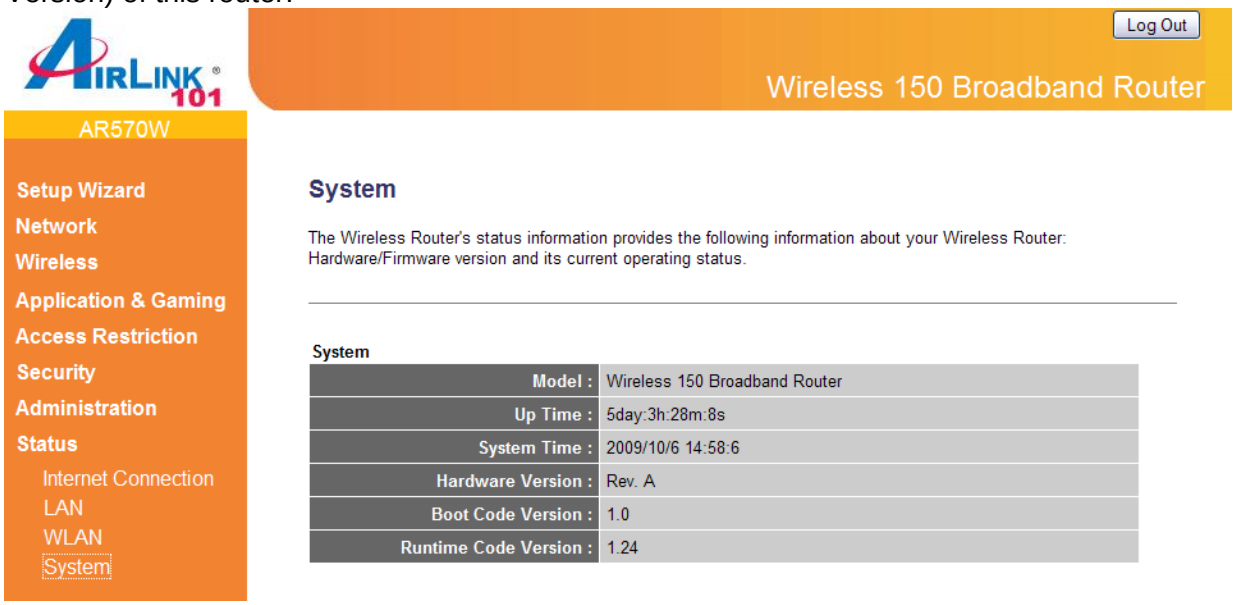
3.7.3 WLAN (Wireless LAN) Status

You can use this function to show the Wireless LAN status of your router, including ESSID (the name of your wireless network), Channel number, and Security.



3.7.4 System Status

You can use this function to know the system information and firmware version (Runtime Code Version) of this router.



Technical Support

E-mail: support@airlink101.com

Toll Free: 1-888-746-3238

Website: www.airlink101.com

*Theoretical maximum wireless signal rate derived from IEEE standard 802.11 specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, mix of wireless products used, radio frequency interference (e.g., cordless telephones and microwaves) as well as network overhead lower actual data throughput rate. This product is based on IEEE draft 802.11n technology and is not guaranteed to be compatible with future versions of IEEE 802.11n specification. Compatibility with draft 802.11n devices from other manufacturers is not guaranteed. Specifications are subject to change without notice. Photo of product may not reflect actual content. All products and trademarks are the property of their respective owners. Copyright© 2009 Airlink101®